



Cyber Readiness:

A Nationally Representative Multi-Mode Survey

Results

Overview of Methodology

Consumer Reports fielded this survey in the spring of 2026 to understand consumers' cybersecurity habits and beliefs, their exposure to scam attempts, and the extent of their losses to scams and account takeovers. These results are based on interviews conducted from March 13th – April 10th, 2026.

The survey was administered by NORC at the University of Chicago through its AmeriSpeak® Panel to a nationally representative sample. Interviews were administered both online and by phone. In total NORC collected 4,682 interviews, 4,482 by web mode and 200 by phone mode, 4,509 in English and 173 in Spanish. Final data are weighted by age, gender, race/Hispanic ethnicity, housing tenure, telephone status, education, and Census Division to be proportionally representative of the US adult population.

Key demographic characteristics (after weighting is applied) of this sample are presented below:

52% female; median age of 47 years old; 60% white, non-Hispanic; 36% 4-year college graduates; and 64% have a household income of \$50,000 or more.

The margin of error for results based on the total sample is +/- 1.91 percentage points at the 95% confidence level. Smaller subgroups will have larger error margins, and only those subgroups for which there are at least 100 unweighted cases are included.

TOPLINE RESULTS

The questions presented below were shown to respondents in this order unless otherwise noted. Where appropriate, question wording, response answer choices, or direction of scales were randomized or rotated and those instances are noted below.

Also shown, where available, are trends over time. Not every item was asked in previous surveys, and where minor revisions to the wording of an item or response choices were made, they are noted below. Note these changes may impact comparability of results.

Prepared by CR Survey Research Department, July 2026

www.cr.org

Survey Notes for Monthly Trends

April 2025 results are based on interviews conducted from April 10 – 21, 2025 with a nationally representative sample of 2,158 US adults.

April 2024 results are based on interviews conducted from April 5 – 15, 2024 with a nationally representative sample of 2,042 US adults.

CONTEXT AND BACKGROUND

INTRO_NODE

This survey is about things you might do to keep your money and identity safe online. Please answer every question honestly; if you are not comfortable answering a question, you can skip it.

CONTEXT1.

In the past 12 months, have you taken a mandatory cybersecurity training for work or school?

This would be a class or video about staying safe online, such as how to protect your passwords or avoid scams.

	Total
	%
Yes	32
No	65
Unsure	3
Base: All respondents	4,676

CONTEXT2.

Do you currently use any social media? These are websites or apps such as Facebook, Instagram, X (formerly Twitter), TikTok, SnapChat, Pinterest, or Reddit.

By "use," we mean look at them at least once every two weeks.

	Cyber Readiness 2026	April 2025 AES	April 2024 AES
	%	%	%
Yes	88	84	83
No	12	16	17
Base: All respondents	4,658	2,158	2,040

CONTEXT3.

How often, if at all, do you order products online?

	Total
	%
Every day	8
Less often than every day, but more than once a week	15
Once a week	17
Less often than once a week, but more than once a month	26
Once a month	14
Less often than once a month	15
I do not order products online anymore, but I have in the past	2
I have never ordered products online	2
Base: All respondents	4,669

CONTEXT4. [RESPONDENTS WERE PROMPTED ONCE TO RESPOND IF THEY DID NOT DO SO INITIALLY. RESPONDENTS COULD SELECT UP TO TWO RESPONSES. RANDOMIZE RESPONSE OPTIONS, HOLDING "OTHER" AT END.]

Which of the following payment methods do you use most often, either online or in person?

Select up to two.

	Total
	%
Credit card	57
Debit card	44
Digital wallet, such as Apple Wallet or Google Pay	19
Cash	13
Prepaid cards or gift cards	7
Peer-to-peer payment services such as Venmo or Zelle	5
EBT cards	4
Buy Now, Pay Later services, like Klarna or Affirm	4
Bank transfers	3
Checks	2
Other, please specify	2
Base: All respondents	4,682

CONTEXT4B. [SHOW IF "DIGITAL WALLET, SUCH AS APPLE WALLET OR GOOGLE PAY" SELECTED IN CONTEXT4. RANDOMIZE RESPONSE OPTIONS, HOLDING "OTHER" AND "DON'T RECALL" AT END IN THAT ORDER.]

You said that your digital wallet is one of your most common payment methods. Like a physical wallet, digital wallets hold different payment types.

When you pay with a digital wallet, which payment type do you use most often?

	Total
	%
Credit card	41
Debit card	36
Linked bank account, such as a checking account	9
Cryptocurrency, such as Bitcoin, Ethereum, or Tether	1
Money stored in the wallet itself, such as a balance in PayPal, Cash App, or Venmo	12
Other	1
Don't recall	1
Base: Respondents who use digital wallets as one of their most common payment methods	889

CONTEXT4 ADJUSTED. [CALCULATED VALUES RECODING RESPONSES IN CONTEXT4 FOR THOSE WHO SELECTED "DIGITAL WALLET," BASED ON SUBSEQUENT RESPONSES IN CONTEXT4B.]

Most frequently used payment types from CONTEXT4, adjusting for responses to CONTEXT4B.

	Total
	%
Credit card including responses from CONTEXT4B	59
Debit card including responses from CONTEXT4B	47
Cash	13
Prepaid cards or gift cards	7
Peer-to-peer payment services such as Venmo or Zelle	5
Bank transfers, including "linked bank account" from CONTEXT4B	5
EBT cards	4
Buy Now, Pay Later services, like Klarna or Affirm	4
Digital wallet, such as Apple Wallet or Google Pay (<i>excluding</i> those who went on to specify they use credit or debit cards or bank transfers through the digital wallet most often)	3
Checks	2
Other, please specify	2
Base: All respondents	4,682

CONTEXT5. [ROTATE RESPONSE SCALE.]

How confident, if at all, do you generally feel using computers, smartphones, or other electronic devices in your daily life?

	Total
	%
Very confident	49
Somewhat confident	42
Not too confident	8
Not at all confident	2
Base: All respondents	4,667

CONTEXT6. [RANDOMIZE RESPONSE OPTIONS, HOLDING "OTHER", "UNSURE", AND "I DO NOT HAVE ANY COMPUTERS, SMARTPHONES, OR TABLETS" AT END IN THAT ORDER. "UNSURE" AND "I DO NOT HAVE ANY COMPUTERS, SMARTPHONES, OR TABLETS" WERE EXCLUSIVE.]

Which, if any, of these operating systems do you use on any computers, smartphones, or tablets that you have?

Select all that apply.

	Total
	%
Windows	62
iOS, MacOS, or iPadOS (Apple operating systems)	50
Android or ChromeOS (Google operating systems)	45
Linux	4
Other, please specify	0.5
GrapheneOS	0.4
Whonix	0.4
Tails	0.2
CalyxOs	0.2
OpenBSD	0.2
Qubes	0.2
Unsure	2
I do not have any computers, smartphones, or tablets	5
Base: All respondents	4,682

CONTEXT7.

Do you currently work in information technology (IT) or cybersecurity?

	Total
	%
Yes	5
No, but I used to	7
No, I have never worked in IT or a cybersecurity field	88
Base: All respondents	4,668

SAFETY PRECAUTIONS

PRECAUTION_NODE.

The next few questions are about online habits or digital security precautions people may or may not take.

PRECAUTION1. [RANDOMIZE ORDER OF PRECAUTION1, PRECAUTION2, PRECAUTION3, AND PRECAUTION4. WITHIN PRECAUTION1, RANDOMIZE RESPONSE OPTIONS, KEEPING "USE A PASSWORD MANAGER TO GENERATE PASSWORDS" AND "USE A PASSWORD MANAGER TO STORE PASSWORDS TOGETHER IN THAT ORDER; KEEPING "USE A MULTI-FACTOR AUTHENTICATION APP" AND "USE MULTI-FACTOR AUTHENTICATION WITHOUT AN APP" TOGETHER IN THAT ORDER; AND HOLDING "NONE OF THESE" AT END. "NONE OF THESE" WAS EXCLUSIVE.]

Which, if any, of the following do you do regarding passwords and logging in to any of your online accounts, like bank accounts, social media profiles, or email accounts?

Select all that apply.

	Total
	%
Use multi-factor authentication <u>without an app</u> , such as through a phone call, text, or email	44
Use strong passwords--that is, at least 16 characters long and difficult to guess	44
Use a multi-factor authentication <u>app</u> , such as Google Authenticator, Duo Mobile, or Microsoft Authenticator	37
Use a password manager to <u>store</u> passwords	36
Use different passwords for every account	35
Use a passkey--that is, a digital credential tied to a user account, often used instead of a password	30
Write down passwords on paper or in a digital file, such as a Word document	30
Change passwords regularly, such as every six months or more frequently	24
Use a password manager to <u>generate</u> passwords	21
Use a physical security key, such as a Yubikey	3
None of these	7
Base: All respondents	4,682

PRECAUTION2. [RANDOMIZE ORDER OF PRECAUTION1, PRECAUTION2, PRECAUTION3, AND PRECAUTION4. WITHIN PRECAUTION2, RANDOMIZE RESPONSE OPTIONS, KEEPING "INDIVIDUALLY ACCEPT AND RUN SOFTWARE UPDATES" AND "TURN ON AUTOMATIC SOFTWARE UPDATES" TOGETHER IN RANDOM ORDER AND HOLDING "NONE OF THESE" AT END. "NONE OF THESE" WAS EXCLUSIVE.]

Which, if any, of the following do you do to keep your devices, like computers, smartphones, and tablets, secure?

Select all that apply.

	Total
	%
Turn on <u>automatic</u> software updates for at least some types of updates, so that the update installs without you having to click anything	48
Use antivirus software	46
<u>Individually accept and run</u> software updates as soon as they are available for at least some types of updates	35
Change passwords on devices that come with default ones, such as baby monitors or routers	35
Use an operating system I believe is more secure	30
Turn off Bluetooth or contactless features, like tap-to-pay	20
None of these	13
Base: All respondents	4,682

PRECAUTION3. [RANDOMIZE ORDER OF PRECAUTION1, PRECAUTION2, PRECAUTION3, AND PRECAUTION4. WITHIN PRECAUTION3, RANDOMIZE RESPONSE OPTIONS, HOLDING "NONE OF THESE" AT END. "NONE OF THESE" WAS EXCLUSIVE.]

Which, if any, of the following do you do to make sure that you only interact with legitimate links, messages, or websites?

Select all that apply.

	Total
	%
Inspect emails and texts before opening <u>links</u> sent in them to make sure they look legitimate	69
Block texts from unknown numbers or emails from unknown addresses (or report them as spam)	67
Inspect emails to make sure they look legitimate before downloading or opening any <u>attachments</u>	67
Examine the sender, preview text, and subject line of emails and texts before opening them and delete them without opening if I find them suspicious	63
Check that there is an icon in the address bar showing the site is secure	38
Only scan QR codes I believe are from a legitimate source, such as in a magazine or on a restaurant table	35
None of these	8
Base: All respondents	4,682

PRECAUTION4. [RANDOMIZE ORDER OF PRECAUTION1, PRECAUTION2, PRECAUTION3, AND PRECAUTION4. WITHIN PRECAUTION4, RANDOMIZE RESPONSE OPTIONS, KEEPING "CLEAR BROWSER COOKIES REGULARLY" AND "ONLY ACCEPT NECESSARY BROWSER COOKIES" TOGETHER IN RANDOM ORDER AND HOLDING "NONE OF THESE" AT END. "NONE OF THESE" WAS EXCLUSIVE.]

Which, if any, of the following safety measures do you take to avoid scams or malware?

Select all that apply.

	Total
	%
Only accept necessary browser cookies	52
Charge devices from their own chargers rather than public USB ports	48
Clear browser cookies regularly	39
Use a VPN when using public WiFi	21
Have a code or safeword with family members to confirm if a call or message is really from them	13
None of these	17
Base: All respondents	4,682

EXPERIENCES WITH SCAM AND TAKEOVER ATTEMPTS

HAPPEN_NODE.

The next few questions are about your experiences with attempted digital scams or cyberattacks.

A cyberattack or digital scam is when someone uses technology to try to harm, steal from, or deceive people online. This can include hacking, fake messages or links, malware, or online shopping scams.

CONTEXT8. [ROTATE RESPONSE SCALE.]

How confident, if at all, are you that you can recognize and avoid a digital scam?	
	Total
	%
Very confident	23
Somewhat confident	60
Not too confident	13
Not at all confident	4
Base: All respondents	4,647

ATTACK1. [RESPONDENTS WERE PROMPTED ONCE TO RESPOND IF THEY DID NOT DO SO INITIALLY. GRID ITEMS WERE RANDOMIZED, KEEPING "RECEIVED AN EMAIL OR TEXT TRYING TO GET YOU TO CLICK A LINK OR DOWNLOAD AN ATTACHMENT" AND "RECEIVED AN UNEXPECTED SPAM MESSAGE " TOGETHER IN RANDOM ORDER; KEEPING "SCAMMER PRETENDED TO BE A PERSON I KNOW" AND "SCAMMER PRETENDED TO BE ASSOCIATED WITH AN ORGANIZATION LIKE . . ." TOGETHER IN RANDOM ORDER; AND HOLDING "OTHER" AT END.]

Which, if any, of the following types of cyberattack or digital scam attempts have you ever personally encountered?

Please include attempts that did not succeed.

	Total
	%
Any "Yes"	91
Base: All respondents	4,682
<i>Received an unexpected spam message--that is, a text, email, call, or social media message--from someone I <u>did not know</u></i>	
	%
Yes	78
No	17
Unsure	5
Base: All respondents	4,671
<i>Received an email or text trying to get me to <u>click a link or download an attachment</u>, such as a fake invoice, job offer, or shipping notice</i>	
	%
Yes	77
No	18
Unsure	5
Base: All respondents	4,672
<i>Received a bill or invoice for something I never ordered</i>	
	%
Yes	55
No	40
Unsure	5
Base: All respondents	4,670
<i>Scammer pretended to be associated with an organization like my bank or the IRS, such as by text, email, or voicemail</i>	
	%
Yes	55
No	40
Unsure	5
Base: All respondents	4,668

ATTACK1. [CONTINUED.]

Scammer pretended to be a person I know, such as by text, email, or voicemail	
	%
Yes	36
No	58
Unsure	6
Base: All respondents	4,670
Was offered a fake online investment opportunity	
	%
Yes	34
No	57
Unsure	10
Base: All respondents	4,671
Bought a product online that never arrived	
	%
Yes	29
No	65
Unsure	6
Base: All respondents	4,668
Received a request for donations that turned out to be fake	
	%
Yes	28
No	59
Unsure	13
Base: All respondents	4,667
Bought a product online that turned out to be counterfeit or defective, or the advertising was deceptive	
	%
Yes	27
No	68
Unsure	6
Base: All respondents	4,671

ATTACK1. [CONTINUED.]

Scammer pretended to be interested in a romantic relationship, such as by text, email, or voicemail	
	%
Yes	26
No	68
Unsure	5
Base: All respondents	4,670
Had my computer or files locked with a demand for money to unlock it (ransomware)	
	%
Yes	9
No	86
Unsure	5
Base: All respondents	4,672
Other, please specify	
	%
Yes	3
No	75
Unsure	18
[No response]	4
Base: All respondents	4,682

ATTACK2. [RESPONDENTS WERE PROMPTED ONCE TO RESPOND IF THEY DID NOT DO SO INITIALLY. RANDOMIZE RESPONSE OPTIONS, HOLDING "YES, ANOTHER TYPE OF ACCOUNT, PLEASE SPECIFY" AND "NO, NONE OF MY ACCOUNTS HAVE EVER BEEN TAKEN OVER THIS WAY, AS FAR AS I KNOW" AT END IN THAT ORDER. "NO, NONE OF MY ACCOUNTS HAVE EVER BEEN TAKEN OVER THIS WAY, AS FAR AS I KNOW" WAS EXCLUSIVE.]

Sometimes hackers or scammers take over people's online accounts and use them to post or send messages while pretending to be the account owner.

Have you ever had an online account taken over in this way?

Select all that apply.

	Total
	%
Yes, a social media account	14
Yes, an email account	8
Yes, an Amazon or other shopping account	4
Yes, a video game account, such as Xbox or Steam profiles	3
Yes, another type of account, please specify	2
No, none of my accounts have ever been taken over this way, as far as I know	75
Base: All respondents	4,682

ATTACK3. [RESPONDENTS WERE PROMPTED ONCE TO RESPOND IF THEY DID NOT DO SO INITIALLY. RANDOMIZE RESPONSE OPTIONS, KEEPING "YES, A BANK ACCOUNT" AND "YES, AN INVESTMENT OR RETIREMENT ACCOUNT" TOGETHER IN RANDOM ORDER AND HOLDING "YES, ANOTHER TYPE OF ACCOUNT, PLEASE SPECIFY" AND "NO, NONE OF MY ACCOUNTS HAVE EVER BEEN TAKEN OVER THIS WAY, AS FAR AS I KNOW" AT END IN THAT ORDER. "NO, NONE OF MY ACCOUNTS HAVE EVER BEEN TAKEN OVER THIS WAY" WAS EXCLUSIVE.]

Hackers and scammers can also take over accounts that do not have posting or messaging, such as bank accounts or streaming services. In this kind of takeover, the scammer does not pretend to be the account owner, but simply uses the account.

Have you ever had an online account taken over in this way?

Select all that apply.

	Total
	%
Yes, a bank account	7
Yes, a streaming service like Netflix or Hulu	4
Yes, a peer-to-peer payment account such as Venmo or Cash App	2
Yes, a store or travel rewards account, like for Target or Delta	2
Yes, a food delivery account like Seamless or Uber Eats	2
Yes, an investment or retirement account	1
Yes, another type of account, please specify	2
No, none of my accounts have ever been taken over this way, as far as I know	84
Base: All respondents	4,682

ATTACK4. [SHOW IF ANY "YES" OPTION SELECTED IN ATTACK2 OR ATTACK3. RANDOMIZE RESPONSE OPTIONS, HOLDING "I'M NOT SURE HOW THEY GOT ACCESS" AT END. "I'M NOT SURE HOW THEY GOT ACCESS" WAS EXCLUSIVE.]

You said that one or more of your online accounts was taken over. We're sorry that happened.

Do you remember how the person got access to your account?

Your answer will help us understand how account takeovers happen, but you don't have to answer if this feels too sensitive.

If more than one account was taken over, select all that apply.

	Total
	%
Someone got into the account without me sharing any information, such as by hacking	34
Someone tricked or scammed me into revealing login information, such as a password or username	13
Someone used a device where I was already logged in, such as a public computer	6
I'm not sure how they got access	48
Base: Respondents who had an account taken over	1,436

ENDNOSCAM. [SHOW IF THERE ARE NO "YES" RESPONSES IN ALL OF ATTACK1 AND "SOMEONE TRICKED OR SCAMMED ME INTO REVEALING LOGIN INFORMATION" NOT SELECTED IN ATTACK4. RESPONDENTS WHO SEE THIS INFO NODE PROCEED DIRECTLY TO THE FINAL QUESTION OF THE SURVEY.]

Thank you for taking the time to answer these questions.

Your responses help us understand how common scams are and how people stay safe online.

We have one final question for you.

ATTACK5. [RESPONDENTS WERE PROMPTED ONCE TO RESPOND IF THEY DID NOT DO SO INITIALLY. SHOW IF ANY "YES" OPTION SELECTED IN ATTACK1. "NO, NOT THAT I AM AWARE OF" WAS EXCLUSIVE.]

Have you ever identified a scam or cyberattack attempt and avoided it before losing money or having an account taken over?

Select all that apply.

	Total
	%
Yes, I recognized it immediately	43
Yes, I did not realize it was a scam immediately, but stopped before I lost money or had an account taken over	19
No, not that I am aware of	42
Base: Respondents who ever encountered any scam attempts (ATTACK1)	4,317

ATTACK6. [SHOW IF EITHER "YES" SELECTED IN ATTACK5. RANDOMIZE RESPONSE OPTIONS, HOLDING "OTHER, PLEASE SPECIFY" AND "DON'T RECALL" AT END IN THAT ORDER. "DON'T RECALL" WAS EXCLUSIVE.]

Thinking about any scams or cyberattacks you avoided, which of the following made you suspicious?

Select all that apply.

	Total
	%
It came from an unknown phone number, email address, or social media account	59
Messages contained suspicious spelling or grammar mistakes	55
The email address or web address did not match the company it claimed to be from or the site it claimed to be	51
It pressured me to take action immediately	50
The request was unusual, such as for payment by gift cards, or to send money through a payment app to an unfamiliar account	46
The offer seemed too good to be true	46
My email or text app flagged it as possible spam	43
It asked for personal information, like a Social Security number or password	38
I got a social media friend request that appeared to be from someone I was already friends with	34
The contact method or timing seemed out of character for the person they were imitating	28
A friend or family member said it seemed like a scam	15
Other, please specify	3
Don't recall	3
Base: Respondents who ever identified a scam or cyberattack attempt and avoided it before losing money or having an account taken over	2,543

EXPERIENCES WITH MOST RECENT SCAM ATTEMPT

HAPPEN_NODE2. [SHOW IF ANY "YES" OPTION SELECTED IN ATTACK1 OR IF "SOMEONE TRICKED OR SCAMMED ME INTO REVEALING LOGIN INFORMATION" SELECTED IN ATTACK4.]

If you have encountered more than one cyberattack or digital scam, please answer the next few questions about the most recent one.

SCAM1. [SHOW IF ANY "YES" SELECTED IN ATTACK1 OR IF "SOMEONE TRICKED OR SCAMMED ME INTO REVEALING LOGIN INFORMATION" SELECTED IN ATTACK4. RANDOMIZE RESPONSE OPTIONS, HOLDING "OTHER, PLEASE SPECIFY" AND "UNSURE" AT END IN THAT ORDER.]

What type of platform did the cyberattack or scam begin on?			
	Cyber Readiness 2026	April 2025 AES	April 2024 AES
	%	%	%
Email	29	27	30
Text message or messaging app like iMessage, WhatsApp, or Facebook Messenger	18	30	20
Phone call	11	11	9
Social media	10	17	23
Dating app or website	2	3	3
Other, please specify	3	6	7
Unsure	21	5	9
[No response]	5	-	-
Base: Respondents who experienced any attack attempt (all three surveys) or had an account taken over because someone tricked them into revealing login information (Cyber Readiness 2026 only)	4,325	1,053	958

Note: Prior to 2026, response options for text message, phone call, and dating app read "a text message," "a phone call," and "a dating app."

SCAM2. [SHOW IF ANY "YES" SELECTED IN ATTACK1 OR IF "SOMEONE TRICKED OR SCAMMED ME INTO REVEALING LOGIN INFORMATION" SELECTED IN ATTACK4. RANDOMIZE RESPONSE OPTIONS, KEEPING "USED A FAKE OR ALTERED VIDEO OR AUDIO TO PRETEND TO BE SOMEONE ELSE", "PRETENDED TO BE SOMEONE I KNOW", AND "PRETENDED TO BE A FAMOUS PERSON" TOGETHER IN RANDOM ORDER; KEEPING "TRIED TO TRICK YOU INTO GIVING PERSONAL INFORMATION, LIKE A PASSWORD OR A CREDIT CARD NUMBER" AND "TRIED TO TRICK YOU INTO SENDING MONEY OR GIFT CARDS" TOGETHER IN RANDOM ORDER; KEEPING "PRETENDED TO BE TECH SUPPORT", "PRETENDED TO BE MY BANK OR CREDIT CARD COMPANY", AND "PRETENDED TO BE A SERVICE I USE BESIDES A BANK, CREDIT CARD COMPANY, OR TECH SUPPORT" TOGETHER IN RANDOM ORDER; AND HOLDING "OTHER, PLEASE SPECIFY" AT END.]

Which, if any, of the following tactics did the cyberattack or scam use?

Remember, please answer only for the most recent scam attempt you have encountered.

Select all that apply.

	Total
	%
Tried to trick me into giving personal information, like a password or a credit card number	24
Tried to trick me into sending money or gift cards	21
Pretended to be a service I use <u>besides</u> a bank, credit card company, or tech support	19
Pretended to be someone I know	17
Pretended to be my bank or credit card company	15
Pretended to be tech support	14
Used a fake online identity to start a relationship with me	8
Used a fake or altered video or audio to pretend to be someone else	5
Took control of my phone number or email address to access my other accounts	4
Locked my files or device and demanded payment to unlock them	4
Pretended to be a famous person	3
Installed monitoring or spying software on my device	3
Other, please specify	10
Base: Respondents who experienced any attack attempt or had an account taken over because someone tricked them into revealing login information	4,325

SCAM3. [SHOW IF ANY "YES" SELECTED IN ATTACK1 OR IF "SOMEONE TRICKED OR SCAMMED YOU INTO REVEALING LOGIN INFORMATION" SELECTED IN ATTACK4.]

Still thinking about the most recent cyberattack or scam attempt you encountered, was it customized using your personal details?

For instance, did it mention personal information like the name of a family member or the last few digits of your bank account number, or did the scammer pretend to be someone you know?

	Total
	%
Yes	20
No	75
[No response]	5
Base: Respondents who experienced any attack attempt or had an account taken over because someone tricked them into revealing login information	4,325

LOSING MONEY TO SCAMS

SCAM4. [SHOW IF ANY "YES" SELECTED IN ATTACK1 OR IF "SOMEONE TRICKED OR SCAMMED ME INTO REVEALING LOGIN INFORMATION" SELECTED IN ATTACK4.]

Have you ever lost money to a cyberattack or a digital scam?

Your answer here will help us understand the amount of harm that these attacks do, but as always, you don't have to answer if this feels too sensitive.

	Total
	%
Yes	11
No	79
I would have lost money, but my payment method allowed me to get it back	8
[No response]	2
Base: Respondents who experienced any attack attempt or had an account taken over because someone tricked them into revealing login information	4,325

ENDNOLOSS. [SHOW IF SCAM4 = "NO" (DID NOT LOSE MONEY). RESPONDENTS WHO SEE THIS INFO NODE PROCEED DIRECTLY TO THE FINAL QUESTION OF THE SURVEY.]

Thank you for taking the time to answer these questions.

Your responses help us understand how people experience and avoid scams, and how to improve protections for everyone.

We have one final question for you.

LOSS_NODE. [SHOW IF "YES" OR "I WOULD HAVE LOST MONEY, BUT MY PAYMENT METHOD ALLOWED ME TO GET IT BACK" SELECTED IN SCAM4.]

We're very sorry to hear that happened. The next few questions will be about the attack or scam that you experienced (or the most recent one, if you have had more than one). Your answers will help us learn about how to prevent scams in the future, but if any questions feel too sensitive you don't have to answer.

SCAM5. [SHOW IF "YES" OR "I WOULD HAVE LOST MONEY, BUT MY PAYMENT METHOD ALLOWED ME TO GET IT BACK" SELECTED IN SCAM4. RANDOMIZE RESPONSE OPTIONS, HOLDING "OTHER, PLEASE SPECIFY" AND "DON'T RECALL" AT END IN THAT ORDER. QUESTION DISPLAYED AS SHOWN IF SCAM4 = "YES" AND AS "YOU SAID THAT YOU WOULD HAVE LOST MONEY IN A CYBERATTACK OR DIGITAL SCAM. HOW WOULD THE MONEY HAVE BEEN TAKEN OR PAID?" IF SCAM4 = "I WOULD HAVE LOST MONEY, BUT"]

You said that you lost money in a cyberattack or digital scam.

How was the money taken or paid?

	Total
	%
Credit card	27
Debit card	25
Peer-to-peer payment services such as Venmo or Zelle	9
Prepaid cards or gift cards	8
Bank transfers	7
Cryptocurrency, such as Bitcoin, Ethereum, or Tether	6
Digital wallet, such as Apple Wallet or Google Pay	5
Cash	2
Checks	1
EBT cards	1
Other	5
Don't recall	5
Base: Respondents who lost (or would have lost) money in a digital scam	809

SCAM6. [SHOW IF "YES" OR "I WOULD HAVE LOST MONEY, BUT MY PAYMENT METHOD ALLOWED ME TO GET IT BACK" SELECTED IN SCAM4. QUESTION DISPLAYED AS SHOWN IF SCAM4 = "YES" AND AS "ABOUT HOW MUCH MONEY WOULD YOU HAVE LOST IN THAT ATTACK?" IF SCAM4 = "I WOULD HAVE LOST MONEY, BUT"]

About how much money did you lose in that attack?

	Total
	%
\$1 to \$49	12
\$50 to \$99	18
\$100 to \$249	20
\$250 to \$499	14
\$500 to \$999	12
\$1,000 to \$4,999	12
\$5,000 to \$9,999	3
\$10,000 or more	5
Don't recall	5
Base: Respondents who lost (or would have lost) money in a digital scam	809

ENDLOSS. [SHOW IF SCAM4 = "YES" OR "I WOULD HAVE, BUT..." (LOST OR WOULD HAVE LOST MONEY).]

Thank you for sharing your experience. We know these topics can be stressful and difficult to think about.

Your answers will help us better understand how scams happen and how to prevent them in the future.

We have one final question for you.

RESPONSIBILITY

FINAL. [RANDOMIZE RESPONSE OPTIONS, KEEPING "STATE GOVERNMENTS" AND "THE FEDERAL GOVERNMENT" TOGETHER IN RANDOM ORDER AND HOLDING "OTHER" AND "UNSURE" AT END IN THAT ORDER.]

Who do you think should be MOST responsible for protecting Americans from digital scams?

	Total
	%
Companies that own the digital platforms where scams can take place, such as social media, texting apps, or sales platfo	29
The federal government	18
Individual consumers	16
Financial companies, such as credit card companies, banks, or payment apps like Venmo	14
Companies that manufacture digital devices, such as computers and phones	5
State governments	2
Other	2
Unsure	14
Base: All respondents	4,646

CONTACT:

Tess M. Yanisch
Senior Research Associate
Tess.Yanisch@consumer.org