Kickstand

KICKSTAND RESEARCH · OCTOBER 2026

The Sneaky Cyber Translation Gap

What people outside the security industry understand about cybersecurity, and what it means for the marketers trying to reach them.



WHY THIS MATTERS FOR B2B MARKETERS

Your buyer is not your only audience.

You write for CISOs and security teams, and for your product pages that's the right call. But a lot of what a cybersecurity brand needs gets decided by people who have never worked a day in security.

The press audience.
In our experience placing security executives in business and broadcast media, the quote goes to whoever can explain the threat in words the audience already understand.

The rest of the buying committee.
The CFO, the general counsel, and the board approve the budget. They don't necessarily read threat advisories.

Your customers' employees and customers.
They're the ones who get the trainings, the login prompts, and, on a bad day, the breach notice.

Everyone outside the security team is an audience you depend on.

So we measured what they understand. We surveyed 1,055 U.S. adults who have never worked in security, IT, or software, and asked what they know, what they do, and who they trust.

ABOUT THIS STUDY

We asked the people security research usually skips.

Most security research surveys security people. This study screened them out. Every respondent uses the internet daily or near-daily for banking, shopping, work, and email, and none has ever worked in cybersecurity, IT, software, or a related field.

They are the general public. That also makes them a reasonable stand-in for the non-technical people in your deals and inside your customers' organizations.



WHAT WE SET OUT TO ANSWER

Which security terms do people understand, and which ones lose them?

Does people's confidence in their own security skills hold up?

Which security habits stick, and what stops the rest?

What do people want from the companies that hold their data?

EXECUTIVE SUMMARY

Four findings that should change how you write.

4%

Can clearly explain a zero-day attack

64% have never heard the term. **64%** can't explain social engineering, and about a third can't explain ransomware.

94%

Trust an expert more when they use plain language

73% say the way companies and experts talk about cybersecurity is hard to follow. **52%** tune out when the jargon starts.

23%

Could pick out an AI-generated image

We tested the people who said they could spot one. **72%** mistakenly picked the real photo. Confidence runs ahead of ability.

3%

Blame a lack of knowledge for weak passwords

94% agree strong, unique passwords are essential, and only **47%** use them on most accounts. The reasons people give are effort and complacency.

THE BOTTOM LINE

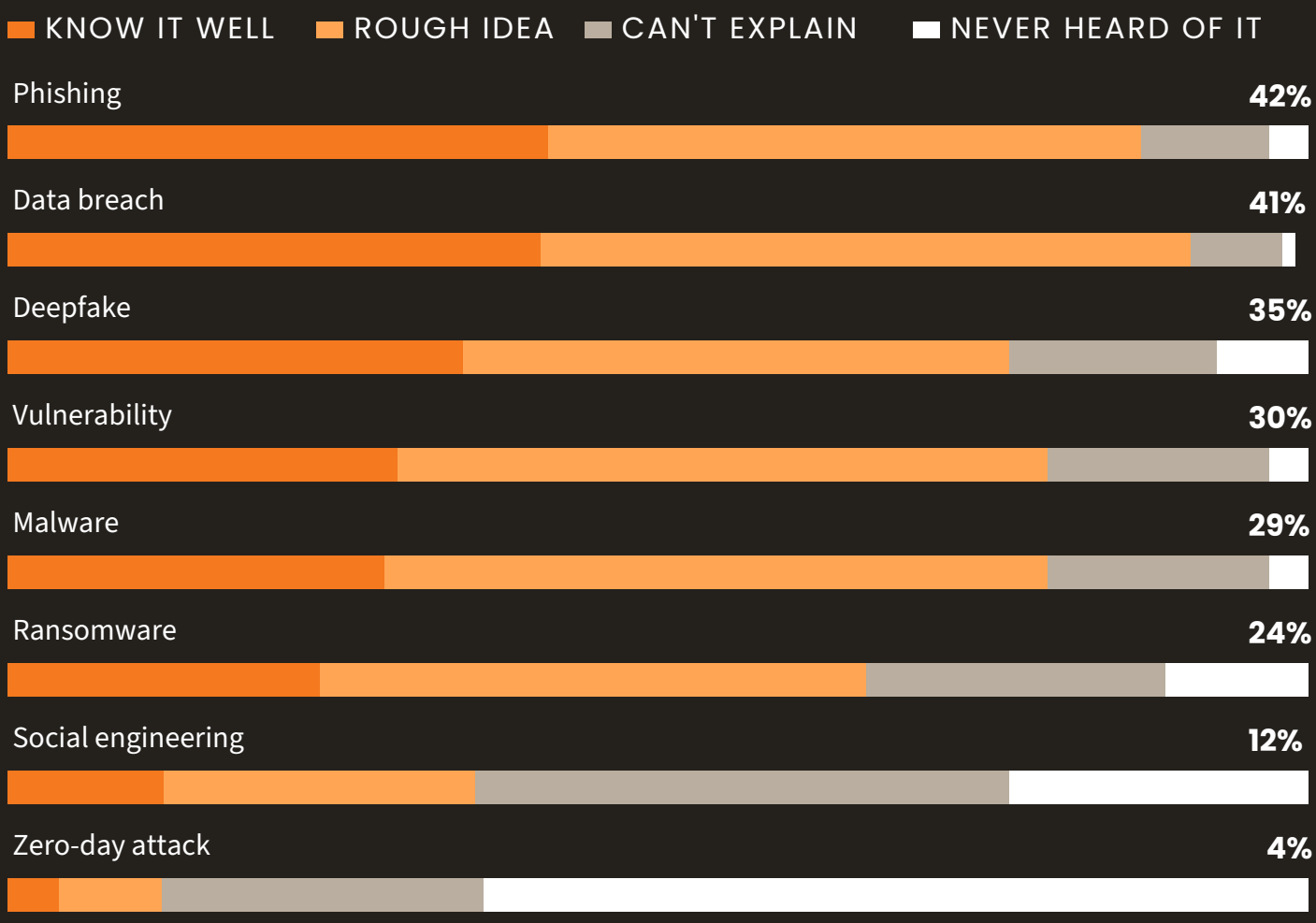
People know security matters and want to do better. What they're missing is a version of the message in their own language and a reason to believe the fix won't be a hassle. **Both are marketing problems**.

01 The vocabulary gap

The industry's core terms fall into three groups: words people know, words they half know, and words that mean nothing to them.

Two of the industry's favorite terms mean nothing to most people.

We asked respondents to rate their understanding of nine threat terms, from "never heard of it" to "know it well and could clearly explain it." Phishing and data breach have made it into everyday language. Zero-day attack and social engineering have not.



64% have never heard of a zero-day attack, and only **4%** could clearly explain one. **64%** have either never heard of social engineering or couldn't say what it means. Even ransomware loses about a third of the audience, who have never heard of it or can't explain it.

Technology terms land better, & people are honest about what they know.

The terms people run into inside products they already use do better. Multi-factor authentication is the best-understood term in the study: **57%** know it well, and only **7%** can't explain it or have never heard of it.

Term	Know It Well	Rough Idea	Can’t Explain	Never Heard Of It
Multi-Factor Authentication	57%	37%	6%	1%
VPN	38%	45%	16%	0%
Cookies	32%	48%	20%	0%
Firewall	30%	49%	21%	1%
Encryption	28%	48%	23%	1%

DID THEY ACTUALLY KNOW IT?

We invited people who said they understood a term to describe it in their own words, then used AI to score the answers for accuracy.

SHARE THAT WERE CORRECT

89% Ransomware
84% Encryption
83% Cookies
63% Zero-day attack

Most people who say they know a term do know it. That matters for reading the rest of this section. When **64%** say they've never heard of a zero-day attack, take them at their word.

Jargon costs you the audience.

73% say the way companies and experts talk about cybersecurity is hard to wrap their head around.

52% tune out messaging that leans on industry jargon. And **94%** are more likely to trust an expert who explains security in plain, everyday terms.

Half of the audience stops listening when the jargon starts, and nearly all of them say plain language is what earns their trust.

Plain language doesn't cost you the sophisticated audience, either. Even among people who call themselves very tech-savvy, **54%** find security talk hard to follow and **86%** trust an expert more for using plain terms.

Jargon Loses the People You Most Need to Reach

The less engaged someone is with security, the more likely jargon is to lose them. **41%** of people who act on breach news tune out jargon-heavy messaging. Among people who'd wait for a breach to hit them directly, it's **59%**. Among those resigned to breaches, **62%**. It's the same story by habit: **34%** of the very proactive tune out jargon, against **74%** of the not very proactive.

And among everyone who tunes out jargon, **96%** say plain language would earn their trust.

What to do with this:

Sort your vocabulary before you write for anyone outside the security team. Based on the share of people who can at least roughly explain each term. Then run the fifth-grader test on anything headed for mainstream press. If a fifth grader couldn't follow why the story matters, it isn't ready to pitch.

PUBLIC UNDERSTANDING	TERMS
Can Use Term Freely	Data breach, phishing, multi-factor authentication
Can Define In Passing	VPN, malware, vulnerability, cookies, firewall, deepfake, encryption
Can Explain Every Time	Ransomware, exploitation
Replace With Plain Words	Social engineering, Zero-day

02 The Confidence Gap

People rate their own security skills highly. When we tested one of those skills, the rating didn't hold up.

Almost everyone thinks they have this handled.

68% rate themselves very or fairly tech-savvy, and only **2%** say they often need help. Confidence about scams runs even higher: **93%** are very or somewhat confident they'd recognize one, and **31%** say a scam would rarely, if ever, get past them.

SELF-REPORTED: HOW TECH-SAVVY ARE YOU?



13%
Very: Others come to me for help



55%
Fairly: I handle most of it myself



30%
Somewhat: I know the basics only



2%
Not very: I often need help

The same people are asking for help. **84%** want to do a better job of keeping their information safe, **58%** wish they understood how, and only **26%** call themselves very proactive about it.

We asked the confident ones to prove it.

73% said they were confident they could recognize an AI-generated image. We showed those 775 people two photographs of flowers, one real and one made with Google Gemini, and asked them to select any they believed were AI-generated. They could pick one image, both, or neither.



REAL IMAGE
72% selected it as AI



AI GENERATED
23% selected it as real

14% of respondents said they beleived both images were real.

The artificial AI confidence issue

The real photograph was picked three times as often as the fake. One pair of images is not a detection benchmark, but fewer than one in four people who called themselves confident picked the image that was actually AI-generated.

More confidence didn't help. **22%** of the very confident picked the AI image, against **23%** of the somewhat confident. The very tech-savvy scored **24%**, the same as the fairly tech-savvy. No generation did meaningfully better than another, with results running from **21%** to **26%**.

A GENERATIONAL PARADOX

25% of Gen Z said they were very confident at identifying AI images, double the **12%** average.

45% of Baby Boomers said they weren't confident, against **27%** overall. On the test it made no difference: **24%** of Gen Z picked the AI image, and so did **25%** of Boomers.



Feeling tech-savvy didn't keep people from getting scammed.

SCAM EXPOSURE

Have fallen victim to an online scam	**12%**
Had a close call	**20%**
Know someone who was scammed	**30%**
Have never fallen for one	**38%**

19% of people who rate themselves very tech-savvy have fallen victim to a scam, against **12%** overall. They may simply spend more time online. Either way, feeling capable didn't protect them.
Scam confidence is highest among people who haven't been tested. **41%** of those who have never fallen for a scam are very confident they'd spot one. Among people who have been scammed, it's **23%**.

Self-reports elsewhere in the survey don't line up either. 84% say they always check that an email or text is legitimate before clicking. Only **55%** say they actively look out for phishing.

Who's Most Sure of Themselves

18% of men call themselves very tech-savvy, against **10%** of women, and **18%** of men say they could clearly explain social engineering, against 8% of women. **40%** of Gen Z are very confident at spotting scams (**31%** overall), and **16%** say phishing isn't a personal concern (**11%** overall). **72%** of Baby Boomers say they actively watch for phishing, against **55%** overall.

What to do with this:

Don't build campaigns on "learn to spot the fake." Most people already believe they can. Give them a step to take instead: verify through a second channel, turn on the setting, use the tool etc.

Don't flatter the audience. "You're too smart to fall for this" is what they already think, and it didn't help the people who thought it most.

Don't assume younger audiences need less explanation. Gen Z reported the most confidence and the least protection. Fewer than four in ten actively watch for phishing, always run antivirus, or install updates right away, against more than half of all respondents. They were also twice as likely as average to have never heard of ransomware (**21%** vs. **11%**).

03 Knowing VS Doing

Nearly everyone agrees on the basics, like strong passwords and prompt updates. Far fewer do them, and the reasons they give are about effort.

Everyone agrees on passwords. Fewer than half follow through.

94% agree that strong, unique passwords are essential. **47%** use them on all or most accounts, **37%** on only some, and **16%** use the same or similar passwords everywhere. Software updates show the same pattern: **90%** agree regular updates keep devices safe, and **53%** install them as soon as they're available.

WHERE PASSWORDS LIVE



Multi-factor authentication follows the same shape. **20%** set it up on their own; **40%** are glad to use it when prompted; **31%** comply only when forced; **7%** actively avoid it.

Two Generations, Two Workarounds

36% of Gen Z use strong, unique passwords on most accounts (**47%** overall), and **22%** reuse the same ones everywhere (**16%** overall). **26%** of Baby Boomers keep passwords on a written note, against **14%** overall. Each found a different way around the same problem.



Why the holdouts hold out.

We asked the 558 people who don't use strong, unique passwords on most accounts what stops them. They could choose more than one reason.

74%	It's difficult to remember multiple passwords
52%	Updating or changing passwords is inconvenient
34%	Creating new passwords takes too much effort
20%	No security issues so far, so it isn't a priority
10%	Don't think it's necessary
3%	Don't know what makes a password strong



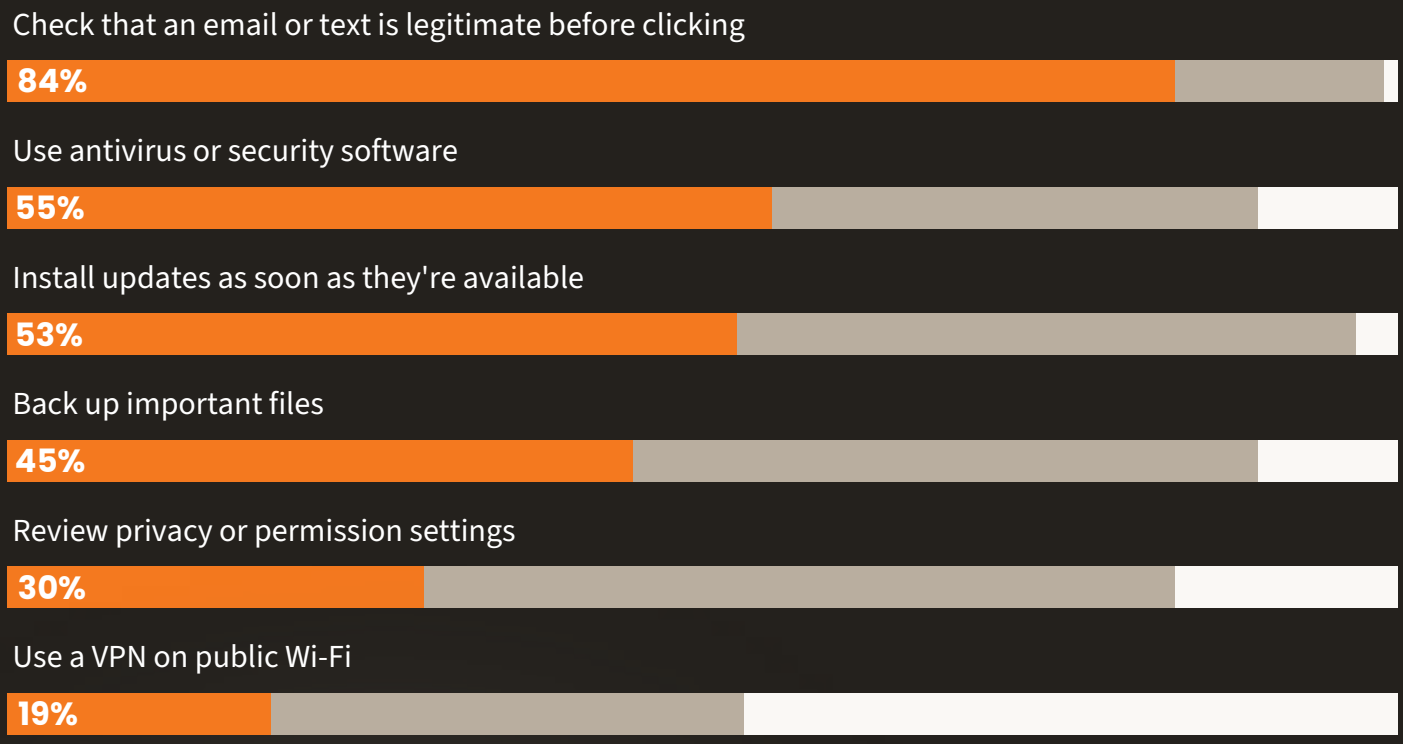
Only 3% said they don't know what makes a password strong.

The top three reasons are about effort. The next two are about not seeing the need.

The more effort a habit takes, the fewer people keep it.

HOW OFTEN DO YOU DO THE FOLLOWING?

ALWAYS SOMETIMES NEVER



Nearly half (**47%**) never use a VPN on public Wi-Fi. Multi-factor authentication shows what does change behavior. Only **20%** set it up on their own, but another **40%** are glad to use it when a site or app prompts them. **31%** use it only when required, and **7%** avoid it. For most people, MFA happens because a product asked for it.

What to do with this:

If your product removes a step, lead with that. "Nothing to remember" and "on by default" answer the objections people actually gave.

Take this data to your product team. You can't claim "on by default" until it's true. The MFA numbers make the case: only **20%** set it up on their own, and another 40% were glad to use it once a product asked.

Stop spending message space proving that security matters. 94% already agree. The argument you need to win is that it won't be a hassle.

Ask for one specific action. Awareness content that asks for general vigilance is asking for the thing people already think they're doing.

04 AI: worried, and using it anyway

The public is already convinced that AI makes attacks worse. It hasn't changed what they do.

THE PUBLIC'S PERCEIVED AI THREAT LEVELS



95%

Expect AI-related scams to become more common



91%

Say AI makes it harder to trust what they see and hear



89%

Say AI is making cyberattacks more sophisticated



76%

Worry AI could impersonate them or someone they know

72% have already encountered a message, call, or video they suspected was AI-generated. None of that has kept people away from the tools.

AI USAGE

Use AI tools on a regular basis	**70%**
Have shared personal info with an AI tool	**46%**
Say the convenience is worth the info shared	**45%**
Worry about how AI companies use that info	**81%**

The Savvy Trade-Off

Self-described very tech-savvy respondents were 26% more likely than average to have shared personal information with an AI tool.

WHAT TO DO WITH THIS

"AI is making attacks more sophisticated" is not a differentiator. 89% of the public already agrees with you. Spend the space on what to do about it.

Make the safe path the easy one. 81% worry about how AI companies use their information, and nearly half share personal information with AI tools anyway. Worry isn't changing behavior. Messaging that asks people to give up a useful tool will lose to messaging that makes the tool safer to use.

05 The trust gap

Most people have been through a breach, and nearly all think cybersecurity matters enough to teach in schools. What they lack is confidence that the companies holding their data are doing their part.

59% say their information has been exposed in a data breach. Another **22%** aren't sure. Only **19%** believe it never has been.

FOUR POSTURES TOWARD BREACHES



47% **Proactive** — acted after hearing about a breach, even when unsure they were affected



28% **Reactive** — a breach would have to hit them directly first



21% **Resigned** — breaches feel inevitable, so they've stopped worrying



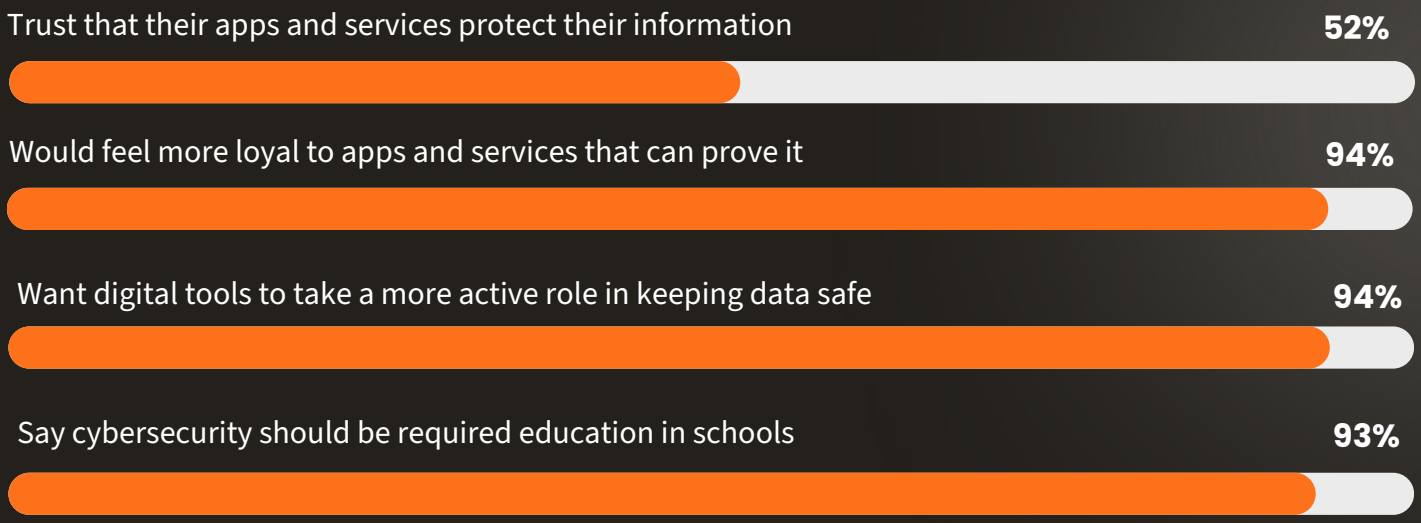
3% **Unconcerned** — don't think about breaches or feel at risk

24% have checked out, either resigned to breaches or unconcerned by them. Another **28%** would act only if a breach hit them directly. Fewer than half act on breach news as a matter of course.

THE YOUNGEST ARE THE LEAST SURE

38% of Gen Z say their information has been exposed in a breach, against **59%** overall, and **34%** aren't sure (**22%** overall). They are also the most likely to wait for a breach to hit them directly before acting: **36%**, against **28%** overall.

93% want cybersecurity taught in schools. Only half trust the apps they already use.



People take this seriously enough to want it taught in schools, and **94%** want the digital tools they use to take a more active role in keeping their data safe. What's missing is trust. Only **52%** believe the apps and services they use are protecting their information, and **94%** say they'd feel more loyal to the ones that can prove it.

That holds even for people who have tuned out. Among respondents who say they're resigned to breaches, **93%** would reward proof and **93%** want their tools to do more. They've stopped worrying, but they haven't stopped wanting better.

WHAT TO DO WITH THIS

Help your customers prove it. Your customers are the "apps and services" in this data. Give them proof they can pass on to their own users in plain language: what's protected, how, and what happens if something goes wrong.

Treat education as a content strategy. 93% want cybersecurity taught in schools, and 58% wish they understood how to keep their own information safe. Plain-language explainers meet a demand people have already voiced.

Write incident communications for the reader who assumes the notice is meaningless. Say what happened, what it means for them, and the one thing to do, in that order.

05 The short version

Five changes to make to your messaging.

Sort your vocabulary

Phishing, data breach, and MFA are safe. Most other terms need a few words of explanation. Zero-day and social engineering need to be replaced with a plain description for anyone outside the security team.

Keep a plain-language version of every story

52% tune out jargon and **94%** trust plain speech more, including **86%** of the very tech-savvy. The plain version is the one that gets you mainstream coverage, and the one your champion can repeat to a CFO.

Sell less effort (not more awareness)

94% already agree passwords matter, and only **3%** of holdouts say they lack the knowledge. Effort is what stops people.

Don’t flatter confident audiences

Self-rated skill didn't predict performance on our image test, and people who call themselves very tech-savvy reported more scams than average. Give people a step to take, and don't tell them they're too smart to be fooled.

Highlight your customers' trustworthiness

Only **52%** trust the apps and services they use to protect them. **94%** say proof would earn their loyalty.

THE BOTTOM LINE

The security industry is fluent in a language most of its audience doesn't speak.

The people in this study know the risks, want to do better, and say they'll trust whoever explains it plainly. The brands that do the translating are the ones in a position to earn the coverage, the internal champions, and the loyalty.

Methodology

Kickstand surveyed 1,055 U.S. adults online from July 29 to August 3, 2026.
To qualify, respondents had to use the internet at least a few times a week for everyday activities such as banking, shopping, email, work, or social media, and could never have worked in cybersecurity, IT, software development, or a related technical field. We also screened out anyone with a household member working for a critical infrastructure organization (healthcare, financial services, government, energy, utilities, or telecommunications). The margin of error for the full sample is approximately ±3 percentage points at a 95% confidence level.

About Kickstand

Kickstand is a global marketing agency with a data-first approach to PR. Our services include media and analyst relations, research, content, crisis communications, and influencer marketing. We help build well-defended market leaders in some of today's most innovative industries, including mobility, robotics, AI, cybersecurity, fintech, insurtech, supply chain and logistics, sales and marketing tech, and eCommerce.

MEETKICKSTAND.COM