

Identity-Theft Questions Overtake Scam Questions on AskTech.Support Ahead of Cybersecurity Awareness Month

Analysis finds identity-theft inquiries rose 10% YOY, as people sought help protecting accounts and personal information they feared were already exposed

SAN FRANCISCO, CA, UNITED STATES, September 29, 2026 /EINPresswire.com/ -- Cybersecurity

“

2026 has been a huge year for data breaches. More than 471 million data-breach victim notices were issued in the first six months of the year—more than during all of 2025.”

AskTech.Support Cybersecurity Expert Dustin Sandlin

advice often starts with how to spot a scam. But as [Cybersecurity Awareness Month](#) begins, questions submitted to [AskTech.Support](#) point to a different concern: What should I do if my identity is already at risk?

In an analysis of 975 cybersecurity-related questions submitted since January 2025, identity theft became the most common topic during January–August 2026. Compared with the same eight months in 2025, identity-theft questions rose 10%, while questions about online scams, phishing and cybercrime fell 34%. Questions about hacked or compromised accounts fell 31%.

The shift suggests consumers may be moving from asking “Is this a scam?” to asking “What do I do now that my personal information or identity may already be compromised?”

That shift comes as identity problems are becoming more complicated for people seeking help. In its [2026 Trends in Identity Report](#), the Identity Theft Resource Center found that 25.6% of people who contacted the organization were dealing with two or more identity incidents, up from 23.5% the prior year. AskTech.Support questions show how those concerns can overlap, with consumers asking about stolen personal information alongside access to their email, phone or bank accounts.

From spotting scams to responding to identity theft

The findings describe what people asked on AskTech.Support and the kind of help consumers are seeking. Questions included how to protect credit after a caller knew someone’s Social Security number, how to regain access to email after suspected identity theft, and what to do when a possible phone compromise coincided with unauthorized bank-account access.

According to AskTech.Support Cybersecurity Expert Dustin Sandlin, the increase in identity-theft questions coincides with an unprecedented volume of personal information being exposed through data breaches.

“2026 has been a huge year for data breaches. *More than 471 million data-breach victim notices were issued in the first six months of the year—more than during all of 2025” said Sandlin. “When your information is stolen in a massive data breach, you often receive no warning that it happened. You may not know your information has been compromised until someone attempts to use it.”

Sandlin said the problem can be particularly difficult for consumers to navigate because there is no single organization responsible for addressing identity theft from beginning to end. A bank may help secure a compromised account or dispute a fraudulent charge, for example, but that addresses only one part of a much larger problem.

“When someone opens a bank account or credit card in your name, there is no central identity-protection authority that can advise you or solve the full problem,” Sandlin said. “Consumers can end up dealing with each individual symptom separately, rather than addressing the broader exposure of their personal information.”

What to do if you think your identity or accounts have been compromised

Sandlin recommends starting with the problem that presents the most immediate risk, then checking where else the information could be used:

1. Freeze your credit files.

A credit freeze can help prevent criminals from opening new credit accounts using stolen personal information.

2. Freeze bank, utility and phone information.

Consumers should also take steps to restrict access to information that could potentially be used to establish or take over financial, utility or telecommunications accounts.

3. Protect government ID accounts.

Consumers should secure their primary government identification accounts to reduce the risk of identity-based fraud.

“Freezing your credit file is a great first step, but simply put, it is not enough,” Sandlin said. “Every adult in the United States should immediately freeze their credit files, as well as their government ID accounts, bank files, phone accounts and utility files.”

Sandlin recommends consumers begin with the resources at FrozenPII (<https://frozenpii.com/>), including its guides for credit, bank, utility and phone freezes and government ID protection.

About AskTech.Support

AskTech.Support connects consumers with verified technology professionals who can provide

personalized answers and guidance on computers, phones, cybersecurity, online accounts and other technology issues. AskTech.Support is part of the JustAnswer network, which has connected consumers with verified professionals since 2003.

*Source: Identity Theft Resource Center 2026 Data Breach Report

Aimee Grove

AskTech.Support

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/945891767>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.