Anybody can be a scam victim... including you

PLEASE NOTE: This transcription was created using an AI transcription tool and may not be a 100% accurate representation of the recorded audio.

[00:00:09] **James Rowe:** You may not want to believe it, but we are all a target for fraud. Including you.

[00:00:18] **James Rowe:** Hello, it's James here in the Witch Studio to bring you another great piece of journalism from one of our magazines. This week I found a piece that was written by Tally Ramsey in the August September issue of witch tech, and it's all about scams. You might think you'll never fall victim to a scam just because some of them seem obvious.

[00:00:39] **James Rowe:** To you, but you could be caught at a bad time or become the subject of manipulation over a lengthy period by a scaled scammer. Here's Tally's piece, adapted for the podcast this week. Read by Tally herself.

[00:01:01] **Tali Ramsey:** It is hard to define who is most likely to become a scam victim. Scam data shows you only which demographics report scams most frequently rather than who's more vulnerable. What the data can show as though is that there's a scam for everyone. Mark Button is a criminology professor. He told me how this works.

[00:01:21] **Tali Ramsey:** Phone scams target older people as they're more likely to use landlines and crypto scams pedals on social media. Appeal to young men who Professor Button describes as being more likely to take risks and be impulsive. The platforms you use can also indicate what types of scams you're most likely to be targeted by, but age can also play a factor of comm's.

[00:01:45] **Tali Ramsey:** Adults Media Lives Study published in May, 2025. Found that when faced with a mockup of a scam, email, people aged over 65 were more adept at spotting the scam than those aged 25 to 34. However, a mockup of a fake social media profile was better spotted by people aged 16 to 24 than those aged over 65 or between 45 and 54.

[00:02:13] **Tali Ramsey:** Action fraud is the National Reporting Center for Fraud and Cybercrime. Its data shows that victims age 60 and over, most commonly report advanced fee scams, where the victim is persuaded to make an upfront payment for goods, services, or investments that never materialize, whereas most younger victims reported online shopping and auction scams where you buy goods that aren't delivered.

[00:02:39] **Tali Ramsey:** So how can anyone be a target? Well, professor Button says it's all about timing,

[00:02:48] **Tali Ramsey:** loneliness and living alone are definitely factors influencing being at greater risk of becoming a scam victim without a network of friends and or family, and no one to ask about potential scams. You don't have a sounding board. He went on the very early stages of cognitive decline. Also put you at greater risk of victimization.

[00:03:10] **Tali Ramsey:** The recently widowed and bereaved are at a very vulnerable stage two, and it's similar with divorce. In fact, our own research has found that scams are often successful when the victims are particularly stressed, tired, or distracted. Scammers then take advantage of this via two primary tactics. They create an overwhelming sense of urgency and manipulate the victim past their bank's warnings and other potential points of intervention.

[00:03:37] **Tali Ramsey:** This is known as social engineering. The data shows that everyone's a target. The ONS revealed that scam victims are spread pretty evenly across the age groups, though there were higher numbers of fraud for those with disabilities compared with those without. For people living in England and Wales, it reported that seven and a half percent of those with disabilities had experienced fraud compared with just 5.3% of non-disabled people.

[00:04:08] **Tali Ramsey:** This doesn't necessarily indicate causation as other factors associated with disabilities such as age can come into play, but scammers do deliberately target people who are at a vulnerable stage in their life. For example, a moderator of a benefits support group on Facebook told us that they had seen a rise in scam text messages claiming to be about cost of living payments.

[00:04:31] **Tali Ramsey:** Likewise, the charity Rethink Mental illness said that it sees comments from scammers appearing under its own social media posts. So what's being done? The Online Safety Act enforced by Ofcom aims to reduce the amount of illegal content online by placing obligations on platforms to detect and remove it, and this includes fraud.

[00:04:56] **Tali Ramsey:** But the process for implementing duties or most paid for fraudulent ads for major platforms was delayed, and most likely won't come into force until 2027. Ofcom told us that the timing of the duties were fraudulent ads under the code. Had changed due to government delays in determining which platforms are subject to these additional duties.

[00:05:19] **Tali Ramsey:** Meanwhile, the payment systems regulator or PSR implemented mandatory reimbursement for bank fraud victims up to a maximum of 85,000 pounds in October last year. Which wants the PSR to maintain its reimbursement scheme when it's reviewed this October, the PSR told us that from the start of the reimbursement policy up until the end of 20 24, 80 6% of money lost to authorized push payments scams or a PP was returned to victims totaling around.

[00:05:54] **Tali Ramsey:** 27 million pounds. It also said that 14% of these claims were made by consumers identified as vulnerable, but that's not good enough, which wants the Online Safety Act to be implemented immediately. The government must use its forthcoming forward strategy to set out a comprehensive approach to tackling fraud, ensuring that there are no gaps in protections that scammers can exploit to target consumers.

[00:06:23] **Tali Ramsey:** In the meantime, be vigilant is the person who they say they are posing as someone you trust. For example, a GP can be how scammers start their social engineering process. If you're contacted by someone official in an unusual way, make sure you double check by making contact through a trusted channel.

[00:06:42] **Tali Ramsey:** Before continuing the conversation, are you being pressured to make a decision? This is one of the most common scam tactic. Fraudsters will try to get you to part with your money and data quickly before you cotton on. Taking some time to slow down and think things through can help you get in touch with your instincts and realize that something is not as it seems, does the person's use of language make you feel overwhelmed or worried?

[00:07:08] **Tali Ramsey:** You may be talking with a scammer if they're using highly emotive language to get you to take a particular action, or they're telling you a sub story even though they just started talking to you. Are you being asked personal questions? Strangers who try to obtain private details about you could be attempting to build up a rapport to eventually scam you.

[00:07:29] **Tali Ramsey:** Fraudsters who create relationships with their victims are typically in it for the long haul and will try to con you out of more and more cash ash. If you or a loved one has fallen victim to a scam, the charity victim support offers emotional support to those affected by crimes including fraud. Visit their website@victimsupport.org.uk.

[00:08:06] **James Rowe:** That brings to an end another podcast from Witch. There's loads more for you to read about everything we discuss today. Just head to the episode description for more useful everyday advice. There you'll also find an exclusive offer for podcast listeners like you to become a witch member for 50% off the usual price, giving you access to our product reviews, our app, one-to-one, personalized buying advice, and every issue of which magazine across the air.

[00:08:28] **James Rowe:** Plus your membership helps us to make life simpler, fairer, and safer for everyone. If you'd like to know when we release a new episode, then make sure you press subscribe wherever you're listening. That way you can be one of the first to listen. And for any questions, comments, or anything in between, follow us on social media at which UK or email us Podcast, at which do co uk goodbye.