AT&T rolls out Wireless Account Lock protection to curb the SIM-swap scourge

AT&T is rolling out a protection that prevents unauthorized changes to mobile accounts as the carrier attempts to fight a costly form of account hijacking that occurs when a scammer swaps out the SIM card belonging to the account holder.

The technique, known as SIM swapping or port-out fraud, has been a scourge that has vexed wireless carriers and their millions of subscribers for years. An indictment filed last year by federal prosecutors alleged that a single SIM swap scheme netted $400 million in cryptocurrency. The stolen funds belonged to dozens of victims who had used their phones for two-factor authentication to cryptocurrency wallets.

Wireless Account Lock debut

A separate scam from 2022 gave unauthorized access to a T-Mobile management platform that subscription resellers, known as mobile virtual network operators, use to provision services to their customers. The threat actor gained access using a SIM swap of a T-Mobile employee, a phishing attack on another T-Mobile employee, and at least one compromise of an unknown origin.

This class of attack has existed for well over a decade, and it became more commonplace amid the irrational exuberance that drove up the price of bitcoin and other cryptocurrencies. In some cases, scammers impersonate existing account holders who want a new phone number for their account. At other times,

they simply bribe the carrier’s employees to make unauthorized changes.

https://arstechnica.com/security/2025/07/att-rolls-out-wireless-account-lock-protection-to-curb-the-sim-swap-scourge/