CYBERSECURITY RISKS CAUSED BY SMS VULNERABILITIES

RISKS IN SMS (TEXT MESSAGING)

SMS messages, commonly referred to as text messages, are still one of the most widely used communications channels for Americans. Millions of users also rely on SMS messaging systems to secure (and access) their email, online banking, social media, or other sensitive accounts, through **one-time passcodes (OTP)** sent via SMS.

Lawmakers have called for prompt action by the Federal Communications Commission (FCC) and other agencies.[i] **So far no agency has taken meaningful responsibility for this problem.**[ii] The FCC has multiple relevant authorities,[iii] but issued a rule that gives carriers flexibility with minimal accountability for securing their networks.[iv]

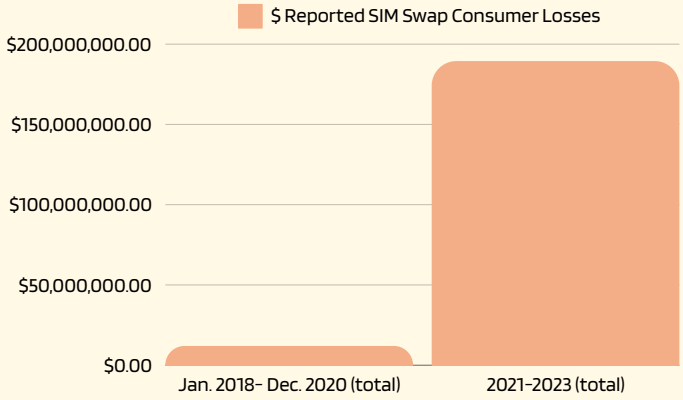
IN A REDIRECT ATTACK...

The bad guy hacks into the phone system and can get copies of messages, eavesdrop on calls, collect location data, and more.*

IN A SIM SWAP ATTACK...

The bad guy transfers your phone service to their device (often by tricking or bribing an employee at your phone company); they then get texts and calls meant for you, including OTP texts.**

SIM SWAP CONSUMER LOSSES



There is a 1,500%+ increase, from approximately $12 million ($12MM) to more than $180MM over a comparable 3-year period. This total reflects reported losses decreasing between 2022 & 2023 ($72MM+ to $48MM+).

LIFE SAVINGS LOST

Most SIM swap victims are "people who are having their life's savings or their child's college savings stolen," rather than the crypto investors that make the news and bring high-profile court cases.[vi]

WHAT YOU CAN DO TO PROTECT YOURSELF

The burden should not be on consumers to pick up the slack for deficient carrier cybersecurity practices, but here are **three steps you can take to protect yourself:**

SIM Freeze, and/or Set a SIM PIN Code
The FCC will soon require all carriers to let customers lock their SIM so their account cannot be transferred, and to unlock and re-lock it any time, for free. Also, you can set a SIM PIN code.[vii]

End-to-End Encrypted (E2EE) Messaging Apps
Use E2EE messaging apps to better guard against a redirect attack.

Authenticator Apps
While some services may force you to use SMS for two-factor authentication (2FA), an authenticator app is more likely to be secure, if you have the option to use one.

WHAT POLICY MAKERS SHOULD DO

Regulators must step in to protect consumers. They can best do so by:

Imposing penalties on carriers who fail to adequately secure their networks.[viii]

Enacting rules that establish minimum cybersecurity requirements.

The Cyber Safety Review Board has called upon the Federal Trade Commission and FCC to "incentivize better security at telecommunications providers by enacting penalties for fraudulent SIM swaps or lax controls."[ix]

https://epic.org/documents/cybersecurity-risks-caused-by-sms-vulnerabilities/

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

*This is generally harder to do on 4G or 5G networks than it was on 3G, but is still possible especially as some systems revert to 3G when connecting a call or transmitting a text message (but not within a web-enabled app).[v]

**SIM swaps can be legitimate—you likely authorize a SIM swap every time you get a new phone and transfer your number and service. However, fraudsters have learned to misuse this process.

WORKS CITED

i *See* Letter from Sen. Ron Wyden to Pres. Biden at 1-2 (Feb. 29, 2024), https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/r.DSbwvU6XD4/v0 [hereinafter "Wyden Letter"]; *see also* Christian Peeters, et al., *SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication*, 22 Procs ASIA CCS 2 (2022), https://dl.acm.org/doi/pdf/10.1145/3488932.3497756 (noting that NIST has publicly recommended that SMS no longer be used to deliver OTPs); Communications Security Reliability and Interoperability Council (CSRIC) VI, Report on Recommendations to Mitigate Security Risks for Diameter Networks 13 (Mar. 2018), https://www.fcc.gov/sites/default/files/csric6report_recommendationstomitigateriskdiamterprotocol032018.pdf; CSRIC VII, Report on Session Initiation Protocol Security Challenges and Mitigation 21 (Mar. 2021), available for download at https://www.fcc.gov/file/20609/download.

ii *See* Wyden Letter at 2.

iii *See, e.g.,* Comments of EPIC, *In re* Public Safety and Homeland Security Bureau Requests Comment on Implementation of Measures to Prevent Location Tracking via the Diameter and Signaling System 7 Security Protocols, PS Docket No. 18-99 at 5-6 n. 33-35 (May 28, 2024), https://epic.org/documents/reply-comment-preventing-location-tracking-via-diameter-and-ss7-request-for-comment/; Reply Comments of EPIC, et al., *In re* Data Breach Reporting Requirements, WC Dkt. No. 22-21 at Section IV (Mar. 24, 2023), https://epic.org/documents/reply-comments-in-re-data-breach-reporting-requirements.

iv *See* Fed. Commc'ns Comm'n, *In re* Protecting Consumers from SIM-Swap and Port-Out Fraud, Final Rule, WC Docket No. 21-341 (Dec. 8, 2023), https://www.federalregister.gov/documents/2023/12/08/2023-26338/protecting-consumers-from-sim-swap-and-port-out-fraud; Reply Comments of EPIC, et al., *In re* Protecting Consumers from SIM-Swap and Port-Out Fraud, WC Docket. No. 21-341 at Sections II, IV (Feb. 12, 2024), https://epic.org/documents/reply-comments-in-protecting-consumers-from-sim-swap-and-port-out-fraud-fnprm.

v *See, e.g.*, Positive Technologies, *Next-Generation Networks, Next Level Cybersecurity Problems* 3 (2017), https://www.ptsecurity.com/upload/iblock/a8e/diameter_research.pdf; Positive Technologies, *Diameter Vulnerabilities Exposure Report* 6-7 (2018), https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf; Mitchell Clark, *Companies can silently reroute your texts to hackers, sometimes for just $16*, The Verge (Mar. 15, 2021), https://www.theverge.com/2021/3/15/22332315/sms-redirect-flaw-exploit-text-message-hijacking-hacking.

vi *See* Busting SIM Swapper and SIM Swap Myths, KrebsonSecurity (Nov. 7, 2018). Sadly, there are many victim stories. *See, e.g.*, Jeremy Jojola, Hacker Steals Man's $24,500 in savings using 'SIM swapper' attack (Mar. 2, 2023), https://www.9news.com/article/news/crime/hacker-sim-card-swap-scam/73-c7f0d7a1-5c90-46f6-b316-7eb2814fe485; Alina Machado, Woman Loses Life Savings in SIM Swap Scam (Aug. 26, 2022), https://www.nbcmiami.com/responds/woman-loses-life-savings-in-sim-swap-scam/2845044/.

vii *See* Fed. Commc'ns Comm'n, Order, WC Docket No. 21-341 (Rel. July 5, 2024), https://docs.fcc.gov/public/attachments/DA-24-649A1.pdf.

viii *See, e.g.*, Fifth Am. Compl. at ¶ 162, *Seth Shapiro v. AT&T Mobility, LLC*, No. 2:19-08972-CBM-RAO (C.D. Cal. Jan. 20, 2023); *Terpin v. AT&T Mobility, LLC*, 399 F. Supp. 3d 1035 (C.D. Cal. 2019) (phone number SIM swapped after provider changed account's security level from "standard" to "extra" and added instructions that representatives should not validate account without new passcode).

ix Cyber Safety Review Board, *Review of the Attacks Associated with Lapsus$ and Related Threat Groups* 37 (July 24, 2023), https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf.

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER