ACCOUNT TAKEOVER FRAUD SCENARIO: SOCIAL MEDIA INFORMATION + SIM SWAP

Scenario Overview

In this scenario, a criminal exploits personal information that Todd shared on social media to determine his mobile carrier and financial institution. The criminal uses this information to socially engineer a customer service representative at a mobile carrier to take control of Todd's phone number, allowing the attacker to complete the financial institution's SMS-based authentication.

Let's take a more detailed look at what happened in this scenario:

SOCIAL MEDIA PROFILE IS USED FOR HARVESTING

1. A criminal purchases personal information about Todd leaked in a third-party data breach. He obtains Todd's full name, phone number, and a username/password combination that Todd previously used for a gaming account.

2. The criminal obtains more information about Todd from reviewing his social media profile and activity. He determines Todd's spouse's full name, Todd's hometown, and date of birth.

3. The criminal sees a post from Todd from a few months ago where he discusses how much he loves the new rewards programs from his financial institution, ABC Bank. He also finds information about Todd's mobile carrier in a comment to another user who was complaining about poor mobile service. Todd's response: "Love my mobile plan with XYZ. You should consider a switch!"

4. The criminal has now determined Todd's financial institution and mobile carrier.

   He attempts to log in to his financial institution account using the leaked username/password combination. He discovers that Todd has reused his password from the other account and that the credential pair is valid. It triggers a one-time authentication request to Todd's financial institution.

SOCIAL ENGINEERING ENABLES SIM SWAP

5. The criminal calls Todd's mobile carrier, pretending to be Todd. He requests a SIM transfer. The customer service representative asks "Todd" to confirm his date of birth and the middle name of his spouse. The criminal answers the questions correctly using information about Todd from his social media profile.

6. The customer service representative performs the SIM transfer. Todd loses mobile service but assumes that it is due to a temporary outage.

7. The criminal again attempts to log in to Todd's account, triggering an OTP request. This time, the request is sent by SMS to the attacker.

8. The attacker completes the OTP request and enters the account. He immediately resets the account password and adds new payees.

9. The next day, Todd tries to log into his mobile banking app but is unable to do so. He contacts his financial institution for assistance.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.