Protecting Your Savings: How to Recognize & Help Prevent Account Takeover Schemes

An account takeover (ATO) occurs when someone uses an individual's stolen personal details to access their online accounts or impersonate them over the phone. After accessing the individual's account or impersonating them, the unauthorized user can withdraw funds, make transactions, lock the individual out of their account, or make purchases.

Methods of Identity Theft

- **Data Breaches** - A security incident where cybercriminals gain full or partial sensitive data.
- **Social Engineering** - Exploitation of human vulnerability to manipulate victims into sharing information, clicking malicious links, or downloading malware.
- **Phishing, Smishing, Vishing, Quishing** - Email, text message, phone call, and QR code attacks used to trick individuals into sharing information, clicking malicious links, or downloading malware.
- **Malware & Keyloggers** - Malicious software that can gain access to accounts via methods like logging all keystrokes and recording login information.

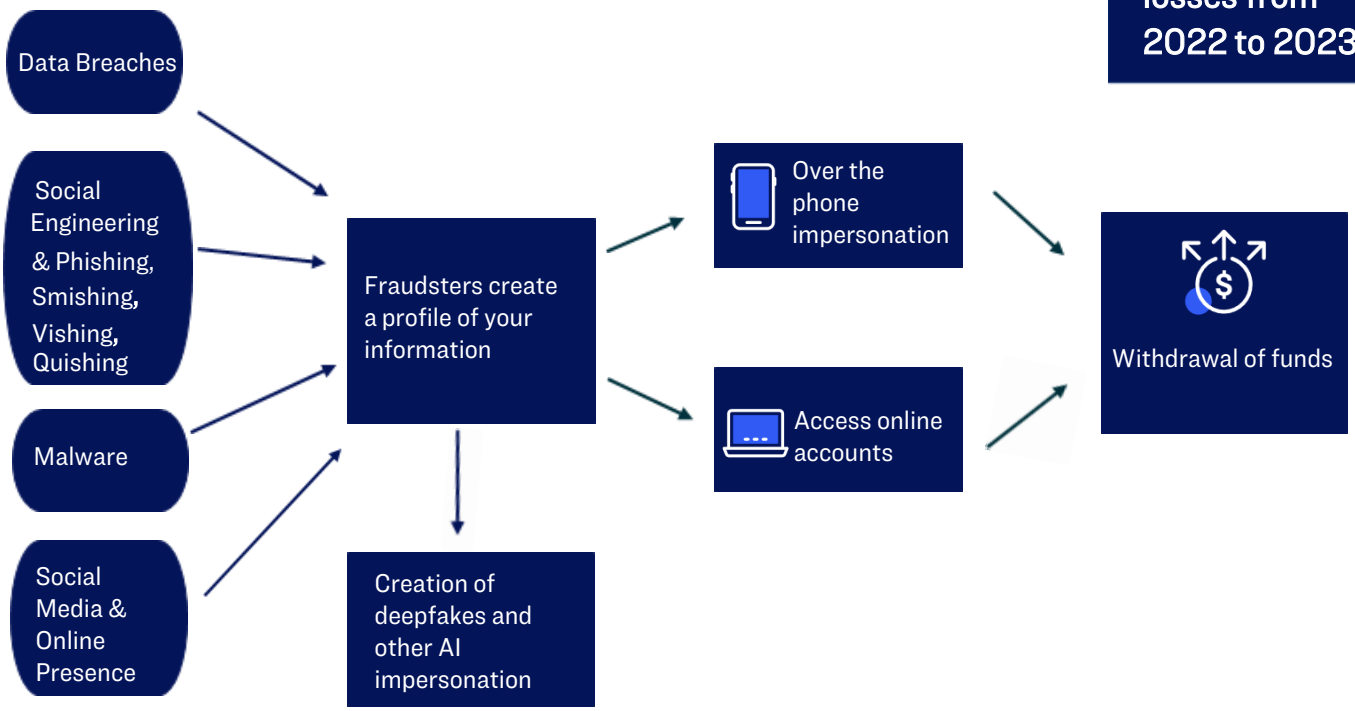
$13 Billion

Lost in ATO attacks in 2023[1]

18%

Increase in ATO losses from 2022 to 2023[1]

How Does an Account Takeover Occur?



[1]AARP, Identity Fraud Cost Americans $43 Billion in 2023, https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html

What Can You Do to Help Protect Yourself?

1.Strong Password Management
- Create complex, long passwords.
- Regularly update, and do not reuse, passwords .

2.Increase Your Account Security
- Use the strongest authentication method available .
- Enable Multi-Factor Authentication .
- Enable push notifications & set up alerts for suspicious activity on your account .

3.Recognize Social Engineering
- Always verify the sender's information.
- Do not click on links and attachments or return unknown calls.
- Use the company's official website to confirm the link or sender's information is real.

4.Use Anti-Virus & Anti-Malware Software
- Use anti-virus & anti-malware software to scan your device for threats.

5.Be Cautious When Using Public Wireless Networks
- Avoid transmitting sensitive information when using public wireless networks .
- Use a virtual private network when possible .

29%

Of people online have experienced ATO attacks[2].

What to Do if Your Account Has Been Compromised

1. Change Your Password
- Change the password of the compromised account and any other accounts with the same password.

2.Report the Fraud to Your Financial Institution
- Notify the financial institution that the compromised account corresponds to.
- If you suspect your TIAA account has been compromised, find reporting information at TIAA.org/security.

3. Consider Freezing Your Credit
- Freeze your credit by phone, mail, or online.
- Contact Equifax at equifax.com or 888-298-0045
- Contact Experian at experian.com or 888-888-397-3742
- Contact TransUnion at transunion.com or 888-888-909-8872.

4. Report the Fraud to the Authorities
- Report fraud to the FTC at reportfraud.ftc.gov or 877-877-382-4357.
- Report identity theft to the FTC at identitytheft.gov or 877-438-4338.
- Report cybercrime to the Internet Crime Complaint Center at ic3.gov.

[2]Security.org, Account Takeovers are Rising: How to Protect Yourself in 2024, https://www.security.org/digital-safety/account-takeover-annual-report/

3867211-0926