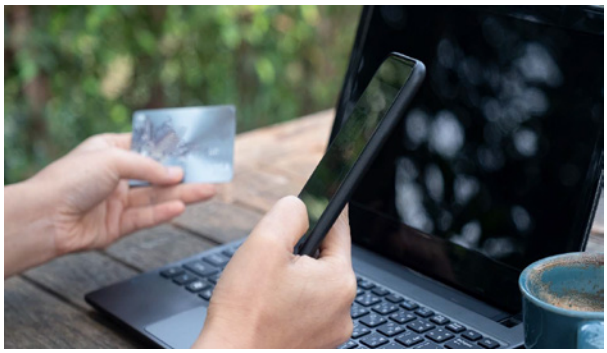
FINANCIAL FRAUD consortium

Industry Insight

5 Ways to Prevent Account Takeover Fraud

Account takeover fraud is a type of cyber-crime or identity theft where a third-party gains access to (or "takes over") an online account, such as an e-mail address, bank account, or social media profile.



Financial ATO includes the thefts of funds from customer accounts as well as accessing portfolios. Common accounts taken over are checking, savings, and credit cards accounts.

Below are some best practices in digital security that can reduce the risk of account takeovers:

1. Employee Education
Train employees on how to recognize phishing attempts, spoof and spam emails and texts, compromised accounts, etc.

2. Login attempt Limits
Limit the number of incorrect login attempts before an account locks. This can help prevent bot spamming, even it it uses multiple IP addresses.

3. WAF configuration
WAF stands for web application firewall. It can recognize account takeover attempts as well botnets and brute-force attacks.

4. IP Block Listing
Many bots use the same IP addresses, you can block these addresses to combat bot attacks.

5. Account Takeover Prevention Software
There are many reputable companies that provide software specifically created to automate the process of detecting account takeovers. FFC member, SpyCloud, is one of these well-respected companies.

Connect with the Financial Fraud Consortium:
info@fraudconsortium.org
(405) 676-1067