5 Ways to Mitigate Account Takeover Attacks

based on industry's best practices

5

Support multi-factor-authentication (MFA)

- Deploy MFA and make it mandatory for all employees.
- Mandate using MFA for partner accounts.
- Avoid using personal mobile phones as a second factor, use USB device token.
- Deploy MFA for customer accounts.

Encrypt credentials' store

- Use a combination of hashing and encryption. At minimum, use bcrypt hashing.

Subscribe to services which detect compromised credentials

- Monitor consistently the credentials that are leaked in data breaches of other online services and can be used to breach your organization - some of your employees and many of your customers will never stop reusing passwords.

Prepare against social engineering attacks with testing and training

- Test your security awareness program and identify real-world social engineering attacks against your organization through social engineering penetration tests.
- Train your employees to identify social engineering attacks based on results from the social engineering penetration test and current market threats.

Monitor the login and account activities to spot bad actors

- Use security information and event management (SIEM) system to monitor login time, frequency, IP address, and other login events to detect suspicious logins.
- Monitor closely the activities of each account for unusual behaviors, anomalies, such as big downloads, privilege escalation, and sensitive data access.
- Define alerts for anomaly activities in SIEM so that it can automatically notify the administrator when an anomaly is detected.

The above checklist was compiled based on the security practices of leading companies, such as Google, Amazon, Microsoft, Twitter, Dropbox, Netflix, Pandora, and OpenTable.