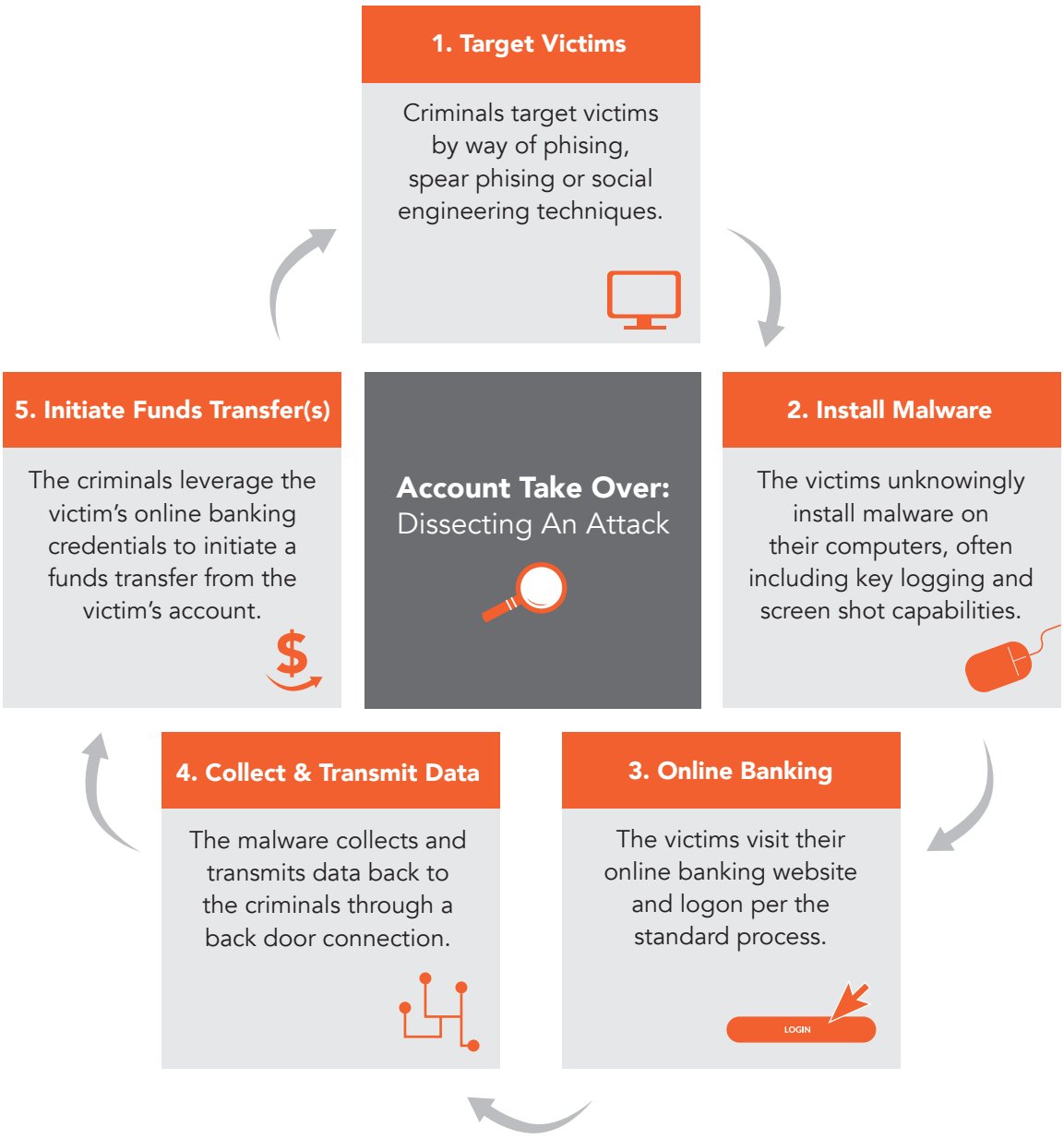
Commercial Account Takeover Fraud Awareness

Account Takeover is a form of identity theft where cyber thieves gain control of a bank account by stealing passwords and other valid credentials. Midland States Bank has implemented procedures to stop or limit cyber fraudsters, however, there are limits to the defenses it can provide. We feel that it is important for customers to take the initiative and implement their own security initiatives and stay vigilant.

How it's done:

Cyber fraudsters use various methods to manipulate or trick victims into divulging personal or account information. They often phish for victims using mass emails, pop-up messages, and/or the use of social networking.



midlandsb.com
855-696-4352

Midland States Bank®

Commercial Account Takeover Fraud Awareness

Protect

- Do not respond to or open attachments or click on links in unsolicited e-mails.
- Midland States Bank will never ask for passwords, credit card numbers, or other sensitive information
- Avoid using the same password for multiple accounts. Make sure you use strong passwords and consider changing passwords regularly.
- Keep your computer/systems patched to protect against software vulnerabilities.
- Install and maintain anti-virus and anti-spyware software to regularly scan your computer.
- Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem. It could be malicious software that allows the fraudster to remotely access and control your computer
- Business Online Banking customers should consider using dual control to validate activities and transactions on the account.
- Do not leave computers with administrative privileges and/or monetary functions unattended.
- Do not use public internet access points to access accounts or personal information.

Detect

- Check account activity regularly for unauthorized transactions and alert the bank as soon as something unusual is detected.
- Pay attention to security emails associated with transactional use or changes to your account profile.
- Run regular virus and malware scans of your computer's hard drive
- Note changes in the performance of your computer such as the following: changes in the way things appear, computer locks up so the user is unable to perform any functions, an unexpected request for a one time password (or token) in the middle of an online session.
- Be on the alert for rogue emails. If someone says they received an email from you that you did not send, you probably have malware on your computer.

Respond

- Immediately contact Midland States Bank so the following actions may be taken:
  - Online access to accounts disabled
  - Online banking passwords changed
  - Open a new account as appropriate
  - Review recent transactions
  - Review online maintenance history
- Follow the instructions for reporting fraud and identity theft from Midland States Bank's Security and Privacy webpage
- Make sure to have a backup plan that covers resolutions for a system infected malware, data corruption, and system/hardware failure
- Consider whether other company or personal data may have been compromised.

midlandsb.com
855-696-4352

Midland States Bank®