



Preventing Corporate Account Takeover

What is Corporate Account Takeover?

Corporate Account Takeover is a form of electronic crime where criminals will use a number of different methods to obtain login credentials to a business online banking account. Those credentials are then used to fraudulently transfer money from the account.

Methods used to obtain login credentials include malicious software, “phishing”, pretending to be someone that business employees trust, and social engineering.

These attacks can result in substantial losses to the business and many times the losses cannot be recovered.

What Can You Do to Protect Your Business Bank Accounts?

While it is not possible to be 100% safe from criminal activity there are a number of things you can do to help protect your business bank accounts.

Computer Security

- 1) Use tools such as firewalls, anti-virus/spyware, and encryption to protect your network from unauthorized access.
- 2) Don't ignore warnings from anti-virus software or firewall devices.
- 3) Use a dedicated computer for online banking and cash management activities. Make sure the dedicated computer is not connected to any other network.
- 4) Block access to high risk websites such as adult entertainment and online gaming.
- 5) Prohibit use of personal email accounts such as Gmail and hotmail.
- 6) Do not conduct online banking activity using unsecured public Wi-Fi.

Employee Education

Employees are the first line of defense in protecting your business bank accounts and should receive regular training.

- 1) Employee training should include cyber security and email best practices.
- 2) Ensure employees never share user ID's or passwords with anyone.



Preventing Corporate Account Takeover

Business Bank Account Security

- 1) Require strong passwords for both business bank accounts and any computers used to access them. Require passwords to be changed frequently.
- 2) Use dual controls for originating and authorizing all ACH and wire transactions.
- 3) Monitor and reconcile online business accounts frequently.
- 4) Review pending and recent ACH and wire transfer activity

If you believe any of your business bank accounts may have been compromised please call Community First Bank at (618)899-5702 as soon as possible.

Additional Resources

Additional Information on preventing corporate account takeover can be found by visiting the following resources:

- 1) Better Business Bureau: 5 Steps to Better Business Cyber Security (<http://www.bbb.org/data-security>)
- 2) Federal Trade Commission: Online Security (<https://www.consumer.ftc.gov/topics/online-security>)
- 3) National Institute of Standards and Technology (NIST): Fundamentals of Information Security for Small Business (<http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf>)
- 4) U.S. Secret Service, FBI, IC3, and FS-ISAC: Fraud Advisory for Businesses: Corporate Account Takeover (<http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf>)
- 5) NACHA Electronic Payments Association: Current Fraud Threats Resource Center (<https://www.nacha.org/content/current-fraud-threats-resource-center>)