BankFive values the relationship we have with you. That's why we want to be sure you have the information you need to safeguard your business. Please take time to review the following Internet Security Best Practices that provide specific guidelines for protecting your business and your bank accounts.

Internet Security Best Practices

Corporate Account Takeover (CATO) continues to be a significant threat to businesses. CATO is a type of fraud where thieves gain access to finances and financial information of a business to conduct unauthorized activities, such as stealing sensitive customer information, illegally transferring funds from the business, and creating and/or adding new fake employees to payroll.

The Massachusetts Office of Consumer Affairs and Business Regulation offers two examples of CATO events on its website. Here are the examples:

- In May 2010, Golden State Bridge, an engineering and construction company based in Martinez, Calif., was robbed of more than $125,000 when cybercriminals hacked into its bank account. The hackers made two automated clearinghouse batch transactions with the office manager's user name and password, routing stolen money to eight other banks across the country. Ann Talbot, Golden State's chief financial officer, learned later that the office manager had violated policy by visiting a social networking site, which the company believed was how her computer was infected with malicious software, or "malware," that antivirus software did not detect. (This information came from a New York Times article).
- A California escrow firm has been forced to take out a high-cost loan to pay back $465,000 that was stolen when hackers hijacked the company's online bank account earlier this year. In March, computer criminals broke into the network of Redondo Beach based Village View Escrow, Inc. and sent 26 consecutive wire transfers to 20 individuals around the world who had no legitimate business with the firm. Owner Michelle Marisco said her financial institution at the time -- Professional Business Bank of Pasadena, Calif. – normally notified her by e-mail each time a new wire was sent out of the company's escrow account. However, the attackers apparently disabled that feature before initiating the fraudulent wires.(This information came from the website, krebsonsecurity.com)

If your business is victimized by CATO, what should you do? Security professionals suggest following these guidelines:

- Immediately shut down computer systems that may be compromised, and disconnect those systems from Internet access.
- Notify BankFive that you suspect your business is the target of a Corporate Account Takeover. If you suspect your business account has been a victim of a Corporate Account Takeover, please contact BankFive at 774-888-6100 AND immediately take the following actions:
    - Disable online access to accounts.
    - Change online banking passwords.
    - Request that the bank's security and auditing departments review all recent transactions and electronic authorizations involving the account(s) in question.
    - Ensure that no one has requested an address change, or re-ordered checks and/or ordered debit cards to be sent to a different address.
- Maintain a written chronology of what happened, what was lost and the steps taken to report the incident to the bank and any other parties, such as authorities and firms that could be impacted. Record the date, time, telephone number, person spoken to, and any other relevant information.
- File a report with the police and any other relevant investigative agency regarding the intrusion. Having a police report on file will help when dealing with the bank, insurance companies, and other parties who have been notified of the fraudulent activity.

To prevent CATO from occurring in the first place, there are steps you can take to protect your business. They include:

- Educate your employees at least annually about online fraud and how to prevent it. Review risky online behavior, such as visiting social media websites and opening unsolicited e-mails and e-mail attachments. Show them examples of suspicious websites and malicious software. New employees should receive this information shortly after joining your company.
- Monitor accounts daily and pay particular attention to wire transfers and ACH transactions.
- Reconcile accounts daily.
- Change passwords at least monthly. Use strong passwords that include a combination of symbols, numbers, and letters. Use a different password for each account. And don't save passwords to a computer.
- Be aware that BankFive will never ask a customer for sensitive information, such as user ID or password for an account, over the phone or in an e-mail.
- Instruct employees to never use a public computer or public Wi-Fi network to access the business's online systems.
- For online banking, use a computer that's dedicated solely for this purpose. The computer should not allow for e-mail or Internet access.
- Log out of computers when not in use.
- Equip all computers with the latest security and anti-virus software.
- Install security updates promptly.

- Ensure that adequate firewalls are in place.
- Do not allow automatic login features, such as those that save login IDs and passwords for future use.
- Restrict administrative rights to computers.

Several resources are available to assist with online security, such as:

- The Massachusetts Office of Consumer Affairs and Business Regulation offers extensive information and resources on CATO: http://www.mass.gov/ocabr/banking-and-finance/laws-and-regulations/dob-faqs/cato08212013.html
- The U.S. Department of Homeland Security offers a wealth of information at: http://www.dhs.gov/publication/stopthinkconnect-small-business-resources
- The U.S. Small Business Administration (SBA) also has a highly informative website at https://www.sba.gov/navigation-structure/cybersecurity
- In addition, the SBA offers an online course entitled "Cybersecurity for Small Businesses" at https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses
- The Federal Communications Commission offers similar information in writing at the following website: https://www.fcc.gov/cyberforsmallbiz

This document is for informational purposes in order to promote business online banking customer awareness and is not intended to provide legal advice. -The best practices included within this document are not an exhaustive list of actions and security threats change constantly.