Business CyberSecurity

What is Corporate Account Takeover?

Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable. The most common attack vectors are email, phone calls/text messages, & malicious websites. Corporate account takeover is a growing threat for small businesses. It is important that businesses understand and prepare for this risk.

Examples of Deceptive Criminal Behavior & Account Holders

- ✓ The FDIC does not directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.
- ✓ Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software in installed, or information is provided.

Employee Education

While having the latest security solution deployed on your network is a great start, the employee is still the most vulnerable part of any network. Businesses should make an effort to educate employees on spotting malicious activity and remaining diligent. If something doesn't look or sound valid further investigation should be encouraged.

Stay Protected

The best way to protect against corporate account takeover is a strong partnership with your financial institution & keeping your network devices (ex. PC) up to date with all security software. Work with your bank to understand security measures needed within the business and to establish safeguards on the accounts that can help the bank identify and prevent unauthorized access to your funds.

A shared responsibility between the bank and the business is the most effective way to prevent corporate account takeover.

dakota western bank Member FDIC EQUAL HOUSING LENDER

How do I find out?

Check your accounts and bank statements each month, and your credit report at least once a year for transactions and accounts you don't recognize. Then act quickly to limit the damage.

What should I do?

Notify all your banks and financial companies as soon as you realize your identity has been stolen or an account is at risk. If you bank with us, call us immediately. We'll work with you to help correct unauthorized transactions in your accounts, fix any incorrect information we've sent to the credit reporting agencies and help protect you from any future identity theft or account fraud.

Prevention Tips

Don't give out financial information such as checking account and credit card numbers on the phone unless you made the call and you know the person or organization you're dealing with.

Don't print your driver's license, phone or Social Security number on your checks.

Report lost or stolen checks immediately. We'll block payment on the check numbers involved. Also, look over new checks to make sure none of them have been stolen in transit.

Store your new and canceled checks in a safe place.

What is Identity Theft?

Identity theft is defined as the fraudulent acquisition and use of a person's private identifying information, usually for financial gain. It happens when a criminal gets your personal information and tries to steal money from your accounts, open new credit cards, apply for loans, rent apartments and commit other crimes—all using your identity. Identity theft can damage your credit, leave you with unwanted bills and require a lot of time and frustration to clean up.

Identity theft can start when someone gets and misuses your personal information such as your name and Social Security number, credit card number or other financial account information.

The thieves might use a variety of methods to steal your information, including:

- ✓ **Skimming:** Stealing credit/debit card numbers by using a special device on ATMs or when processing a purchase
- ✓ **Phishing:** Pretending to be a financial institution or other company and sending email or pop-up messages to get you to reveal your personal information
- ✓ **Pretexting:** Pretending to be you when they call financial institutions, phone companies and other sources to get additional information
- ✓ **Redirecting your mail:** Filling out a change-of-address form to have your billing statements sent to an address they choose
- ✓ **Dumpster diving:** Rummaging through trash looking for bills or other paper with your personal information on it
- ✓ **Social networking:** Thieves regularly troll social networking sites to steal personal information they can use to commit fraud

dakota western bank Member FDIC EQUAL HOUSING LENDER