First County Bank
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

Corporate Account Takeover (CATO)

CATO is a type of fraud where cybercriminals gain unauthorized access to a business account such as email, social media, or bank accounts. CATO is an evolving and rising threat for businesses and can result in direct financial loss, legal and regulatory fees, operational disruption, and reputation damage. Cybercriminals gain access using a wide variety of techniques but there are things you can do to prevent your business from becoming a victim.

CATO Techniques and Warning Signs

Phishing - Fraudsters pose as a legitimate organization and ask for personally identifiable information from the individual or company. Warning signs are Emails that start with generic greetings like “hi there” instead of the recipient’s name, ask you to complete an action almost immediately, that do not take you to a page it claims to, or the URL does not begin with HTTPS.

Brute Force - Cyber criminals attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until one works. Common signs are high login attempts on a single account, failed testing attempts with multiple account ids and passwords, an exponential rise in account locks, and more cases of hijacked accounts.

Password Spraying - A type of brute-force cyberattack where a criminal tries to guess a known user’s password using a list of common, easy-to-guess passwords such as “123456” or “password.” This process is often automated and occurs slowly over time to remain undetected. Warning signs include login attempts from non-existent users, increase in account lockouts, high login failure rate, and repeated login attempts from the same URL.

Credential Stuffing - Hackers obtain user credentials from past data breaches by purchasing them at low cost on the dark web and then develop rudimentary scripts to automatically “stuff” username and password combinations into the login fields of your web applications until a match is found. Signs are irregular traffic volumes, high use of non-existing usernames during authentication, and abnormal bounce rate at authentication.

Man-in-the-middle (MITM) - Criminals exploit weak web-based protocols and insert themselves between entities in a communication channel. None of the parties sending email, texting, or chatting on a video call are aware that an attacker has inserted themselves and is stealing their data. Common signs are TCP and HTTP signatures during user sessions do not match, evil twin Wi-Fi networks like IkeaFreeWiFi and IkeaWiFiJoin in the same location, fake looking login pages or software update pop-ups, and suspicious wireless networks.

Session Hijacking - compromises the session by exploiting a valid web session control mechanism (token), such as a Session ID, to gain unauthorized access to the Web Server. Signs include unusual frequency in the Receiving Signal Strength (RSS).

Social Engineering - An employee is manipulated into giving away login credentials or access to sensitive information. Warning signs include unsolicited emails requesting payment information, asking for One Time Password following a two-factor authentication, suspicious chat box pop ups.

March 26, 2024

Ways to Prevent CATO

Strong Passwords and Multi-Factor Authentication

A strong password is long, complex, and made with a combination of letters, numbers, and symbols. It should also be changed frequently and never be used on more than one account. MFA is an extra security layer. MFA options like a biometric scan or a security token make unauthorized access to an account much harder.

CATO Detection Software

CATO detection software offers account takeover prevention by detecting and blocking unauthorized automated hacking tools.

Employee Training and Education

Training and education should include how to spot phishing emails and fake websites, as well as updating employees on the latest security threats and security best practices. Employee security training should be held regularly.

Secure Third-Party Applications

Review every new application's security features and consider whether you really need the application in the first place. Once you connect to the application, ensure that it's always kept up to date with the latest patches. Additionally, you should monitor the application for suspicious activity or signs of a potential CATO attack.

Access Controls

Only give account access to the right people at the right time, as determined by their job function, best practices, and any compliance requirements. Regularly review and update your access controls to address changes in roles, requirements, or employees that have left the business.

If you have any questions, please call our Customer First Contact Center at (203) 462-4400.

(Monday – Friday (excluding bank holidays) from 8:30 a.m. to 4:30 p.m.)

March 26, 2024