HOW BUSINESS ACCOUNTS MAY BE TARGETED FOR ACCOUNT TAKEOVER FRAUD

HIGHLIGHTS:

- Businesses can be prime targets for account takeovers because they generally hold larger balances than individuals and often involve multiple authorized users, creating more entry points for attackers.
- Harvesting information about a business and its employees is often the first step for committing account takeovers, facilitated by business email compromise and social engineering tactics to enable account access.
- Monetization of business accounts can occur because of direct transfer of funds before detection or by exploiting the often-complex array of relationships that businesses maintain.
- Early reporting of suspicious activity and secure password habits can help address attacks before money is lost.
- Multi-factor authorization, continuous monitoring and employee training may be essential to help protect accounts and reduce risk.

Consumer accounts may most often come to mind when considering account takeover attacks – but business accounts face account takeover threats, too, with potentially much greater monetary impact. Account takeover incidents involving business accounts result in billions of losses each year (Off-site). Organizations typically hold more funds and have higher cash flows than most individual consumers, making them more attractive targets. Additionally, organizations often authorize multiple users to create and approve payments, providing more entry points for social engineering attacks. Criminals exploit this by focusing on "hacking the person" rather than the technology.

This article explores the account takeover risks organizations face and common methods criminals use to target business accounts.

CRIMINALS EXPLOIT COMMON ATTACK VECTORS TO ACCESS BUSINESS ACCOUNTS

Like consumer accounts, business accounts face account takeover risks from data breaches (Off-site). When personal accounts are compromised, stolen credentials often include passwords employees reuse for business logins. These digital artifacts provide attackers with a simple path to validate stolen credentials across sites.

HOW BUSINESS ACCOUNTS MAY BE TARGETED FOR ACCOUNT TAKEOVER FRAUD

Publicly available information also helps attackers harvest data on businesses and employees. Social media and professional networking sites may reveal job titles and responsibilities, helping criminals identify employees with account access. By targeting these individuals, attackers aim to compromise accounts that can authorize or move funds, making them high-value targets.

Criminals also use phone number spoofing (manipulating caller IDs to display a trusted number) to impersonate legitimate financial institution representatives and create urgency to deceive employees. Attackers target employees directly, often through phone calls or emails, posing as executives, IT support or fraud prevention teams. They may claim urgent issues with payment accounts – such as suspected fraud or transaction failures – to create pressure. Criminals may manipulate staff into revealing sensitive information, including one-time passcodes or multi-factor authentication (MFA) credentials, granting them access to high-value business accounts.

Another growing threat is MFA fatigue, when users become overwhelmed by repeated MFA requests and start approving them without verifying their legitimacy. Attackers exploit this by sending dozens – or even hundreds – of approval requests to employees. After being bombarded, employees may click "Yes" out of frustration or confusion, unknowingly granting unauthorized account access to a criminal.

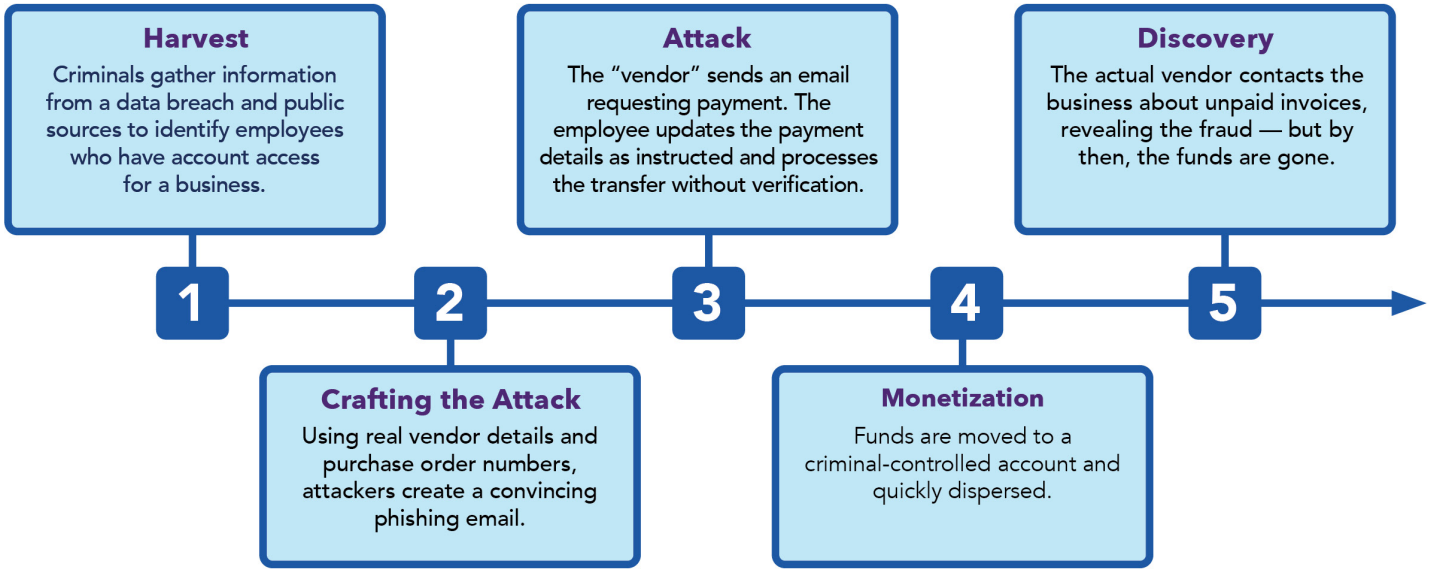
BUSINESS EMAIL COMPROMISE CAN ENABLE BUSINESS ACCOUNT TAKEOVERS

Business email compromise is a major and growing threat. In these schemes, criminals compromise either the sender or receiver in a legitimate business email interaction. They may impersonate executives to send urgent payment requests, issue fraudulent invoices or request account detail changes. These messages often appear to be authentic and come from trusted communication channels, prompting employees to change account details or approve payments without realizing the instructions came from criminals.

Phishing attacks (fraudulent emails) often facilitate business email compromise and go beyond the typical fake text or email. Because companies interact with customers, vendors and financial institutions, attackers aim to create content that looks legitimate – such as fake invoices, payment requests or service updates. These phishing texts or emails are designed to trick employees into clicking links or sharing login details.

HOW BUSINESS ACCOUNTS MAY BE TARGETED FOR ACCOUNT TAKEOVER FRAUD

Account Takeover Through Business Email Compromise



HIGHER CASH FLOWS AND MULTIPLE ENTRY POINTS MAKE BUSINESS ACCOUNTS ATTRACTIVE FRAUD TARGETS

The monetization stage of business account takeover can involve a high level of sophistication because of the businesses' many relationships with customers, vendors and financial institutions. These connections create opportunities for attackers to victimize other individuals or organizations by sending fake invoices or payment requests disguised as normal business operations.

Direct monetization of the account remains another common tactic for criminals. Once inside a business account, attackers can initiate wire transfers, ACH payments or other transactions to drain funds. These transfers often happen quickly and may be routed through multiple accounts or converted into digital assets, making recovery extremely difficult.

The combination of speed, automation and deception means that the money often is gone by the time suspicious activity is detected. This can result in significant financial losses and operational disruptions, including liquidity challenges, missed payroll or vendor payments, and other operational challenges.

HOW BUSINESS ACCOUNTS MAY BE TARGETED FOR ACCOUNT TAKEOVER FRAUD

CONCLUSION: BUILDING A CULTURE OF VIGILANCE

Account takeover attacks on business accounts are as much about people and processes as technology. Businesses can reduce risk by fostering a culture of awareness and verification. Reporting suspicious activity early, such as odd multi-factor authorization prompts or emails, can stop fraud before funds disappear. Strengthening core defenses through multi-factor authorization and unique, complex passwords is important to help protect business accounts from account takeover fraud. Regular reviews and employee training also matter. Combining smart security practices with human vigilance can make account takeover attacks much harder to execute.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, use of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.