NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

Business Email Compromise

What is BEC?
Business Email Compromise, BEC, is a fraud scheme where attackers use compromised business accounts to send fake invoices, financial requests, or requests pertaining to modification of sensitive data. It is a common tactic and impactful to North Dakota businesses.

How does it work?
Attackers first gain access to a business account then pose as trusted partners, requesting payments, payments, confidential information, or changes to account details, aiming to defraud businesses and their clients. BEC can lead to significant financial loss and further compromise business data and other accounts.

Business Email Compromise is a sophisticated form of fraud that can target multiple aspects of a company's financial operations. Attackers may attempt to convince employees into altering payment details for vendors, redirecting funds to fraudulent accounts. Similarly, BEC can attempt deceive your customers into sending payments to the wrong destination by impersonating your business. Even HR departments can be targeted, with attackers attempting to change the direct deposit details for employee paychecks. This wide range of targets makes BEC a highly dangerous and versatile form of financial fraud.

Business Email Compromise (BEC) primarily exploits legitimate but compromised accounts, but attackers may also use domain spoofing or typo squatting to make emails appear as though they are from trusted partners. A common tactic is email thread hijacking, where threat actors insert malicious content into an ongoing conversation, often involving invoices or contracts. This makes the fraudulent request seem more legitimate and increases the chances of success.

How can I protect myself or my company?
Since BEC often is a result of compromised accounts, the best method to prevent against BEC is implementation of multi-factor authentication.

Educate yourself and your employees about business email compromise, how it is carried out, and what threat actors are attempting to gain from this tactic.

Just because a sender or platform is familiar, do not put blind trust in them. If you receive an unexpected file share from a business contact, such as unexpected invoice or contract, verify that it is legitimate with them before opening it.

A non-technical solution to protect against BEC and financial fraud is to require additional non-digital steps for verification before making any changes to account details, routing, or wiring information.

For manufacturers and businesses handling contracts, it may be beneficial to implement a contract requirement for additional verification before any changes to wire instructions for your customers. This extra step helps prevent threat actors from deceiving your customers and reduces the risk of fraudulent payments.

ndslic@nd.gov