Business email compromise can happen to anyone. This is how it works and steps to prevent it.

Fraudster preys on weak password habits and gains access to a business email account.

Fraudster monitors email traffic looking for financial transactions.

When the opportunity arises, the fraudster sends an email from the account asking for funds to be sent somewhere different.

There are automated tools that allow fraudsters to lurk until an opportunity arises.

RECOGNIZE AND PREVENT

BUSINESS EMAIL COMPROMISE

Follow best practices for passwords by using ones that are unique, long, and not easy to guess.

Use MFA or multifactor authentication. This makes it more difficult to hack into an account.

Be vigilant to spot irregularities in language and instructions in emails.

Verify payment instructions directly with the legitimate person by using a known phone number.