DON'T BE A VICTIM OF INTERNET FRAUD

Business E-Mail Compromise (BEC)

WHAT IS A BEC SCAM?

Cyber fraudsters are registering domains that appear to belong to local government entities so they can defraud supply companies.

These domains are used to contact suppliers and order high-value goods such as IT equipment and pharmaceutical chemicals under the government entities name.

FOR EXAMPLE:
Suppliers receive an email claiming to be from a city or county requesting a quotation for goods on extended payment terms. Once the quotation has been provided, a purchase order is emailed to the supplier that is similar to a real purchase order.

The purchase order typically instructs delivery to an address which may or may not be affiliated with the organization.

The items are then received by the criminals, but no payment is ever received by the supplier. In one recent example, fraudsters impersonating one particular local city is estimated to have netted around $350,000 worth of goods in this manner.

DON'T BE A VICTIM:
The business e-mail compromise scam has resulted in companies and organizations losing billions of dollars. But as sophisticated as the fraud is, there is an easy solution to thwart it: face-to-face or voice-to-voice communications.

"The best way to avoid being exploited is to verify the authenticity of requests to send money or products by calling the person in the request and speaking to him or her directly on the phone," said Special Agent Martin Licciardo of the New York FBI. "Don't rely on e-mail alone."

Here are other methods businesses have employed to safeguard against BEC:

- Create an e-mail rule to flag e-mail communications where the "reply" e-mail address is different from the "from" e-mail address shown.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having secondary sign-off by company personnel.
- Confirm requests for transfers of funds or purchase orders by using phone verification as part of a two-factor authentication; use previously known numbers, not the numbers provided in the e-mail request.
- Carefully scrutinize all e-mail requests for fund transfers or purchase orders to determine if the requests are out of the ordinary.

Awareness, internal check and balance procedures, and vigilance are the key methods to combat this type of fraud.

REPORT CYBER CRIME

If you believe you have been a victim of an internet-related crime, report it to these government authorities:

- The Internet Crime Complaint Center (IC3) refers internet-related criminal complaints to federal, state, local, or international law enforcement. Keep in mind, you will need to contact your credit card company directly to notify them if you are disputing unauthorized charges on your card or if you suspect that your credit card number has been compromised. (These complaints are routed directly to the local FBI)
- The Federal Trade Commission (FTC) shares consumer complaints covering a wide range of categories, including online scams, with local, state, federal, and foreign law enforcement partners. It cannot resolve individual complaints, but can give you information on the next steps to take.
- EConsumer.gov accepts complaints about online and related transactions with foreign companies.

The Department of Justice (DOJ) helps you report computer, internet-related, or