First County Bank
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

Business E-mail Compromise

What Is It?

Business E-mail Compromise ("BEC") is among a growing trend in cyber-enabled crimes affecting businesses of all sizes. Unlike corporate account takeover activity where criminals access and conduct transactions directly from the victim's account, BEC involves impersonating the victim and submitting seemingly legitimate transaction instructions.

How Does BEC Occur?

BEC focuses on using compromised e-mail accounts to mislead the financial institution into conducting unauthorized transactions. BEC can be broken down into three stages:

Stage 1 – E-Mail Account is Compromised

Criminals unlawfully access a victim's e-mail account through social engineering or computer intrusion techniques.

Stage 2 – Fraudulent Transaction Instructions are Transmitted

Criminals then use the victim's stolen e-mail information, even using the victim's actual e-mail account, to make fraudulent transaction requests.

Stage 3 – Unauthorized Transaction is Executed

Criminals trick the company's employee or financial institution into conducting what appears to be a legitimate, but is in fact an unauthorized, transaction.

How Can You Protect Your Business from BEC?

Robust e-mail, network, and endpoint security solutions must work alongside user education.

- **Be aware of the RED FLAGS.**
  As with so many phishing schemes, imposter e-mail threats bear common hallmarks:
  - Company leaders ask for unusual information;
  - E-mail recipients are asked to keep the request confidential;
  - Normal accounting procedures are bypassed;
  - Unusual date format and sentence construction suggest that the e-mail was written by a non-native speaker unlike the sender being impersonated;
  - "Reply To" address does not match the sender address.
- **Be Suspicious.**
  Asking for clarification or check with a colleague before executing a transaction.
- **Confirm that the Sender is Genuine.**
  Check the "Reply To" field, the domain accuracy and watch for personal accounts.
- **Encourage Employees to Trust Their Instincts.**
  If something doesn't feel right, it probably isn't.
- **Slow Down.**
  Attackers time their campaigns around busy periods when employees are most likely to move quickly through communications and are less likely to consider the validity of the request.

First County Bank uses stringent verification methods to confirm that transfer requests are from the legitimate representative of the account.
If you have any questions, please feel free to call our
CustomerFirst Contact Center at (203) 462-4400 *(Monday - Friday from 8:30 a.m. to 4:30 p.m.)*

(October 2016)