Topic: Avoid Business Email Compromise Scams

Business email compromise (BEC) – also known as email account compromise – is one of the most financially damaging online crimes, exploding people's reliance to conduct business.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request:

A vendor, our company, regularly deals with sends an updated mailing address

A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. They ask for the serial numbers to email them out.

An employee asked for a deposit via ACH with account and router numbers

False emails with USPS/UPS/FedEx tracking number (check address before clicking on link)

How Criminals Conduct BEC Scams

Spoof an email account or website domain. Slight variations on legitimate addresses to fool victims into thinking fake accounts are authentic.

Sending phishing emails. These messages looks like they're from a trusted sender to trick victims into revealing confidential information

That information lets criminals access company accounts, calendars and other data with personal details to carry out schemes.

Use Malware, where malicious software infiltrate networks to gain access to data information like passwords and financial accounts.

How to Protect Yourself

Don't click on anything in an unsolicited email or text message asking you to update or verify account information.

Use Google search domain names, addresses, phone numbers, or call the company to ask if the request is legitimate

Carefully examine the email address, URL and spelling used in any correspondence.

Be careful what you download. Never open email attachment from someone you don't know.

Be wary of any attachments forwarded to you from anyone.

Set up two-factor (or multifactor) authentication on any account that allows it and never disable it.

Verify payments and purchase requests in person or by phone to make sure they are legitimate or product you brought instead of clicking any link in an email.

Verify any change in account number or payment procedures with the person making the request.

Be especially wary if the requestor is pressing you to act immediately.