Vendor Email Compromise

WATCH OUT FOR A NEW CLASS OF BUSINESS EMAIL COMPROMISE WHEN YOU RECEIVE AND PROCESS INVOICES.

A Vendor Email Compromise (VEC) attack aims to take over the email account of a vendor. This type of scam includes:

- **The VEC group sends phishing emails to the vendor's staff that include a malicious link.**
- **Once the vendors click on the link, they're redirected to a phishing login page where vendors are asked to log in using their credentials.**
- **Once the vendors enter their credentials, the attacker uses those credentials to set a forwarding rule to forward all emails received by the vendors to the attacker's email.**
- **The attacker then monitors the inbox for any emails regarding invoices or payments.**
- **If the attacker notices email that contain invoices or payments, they will duplicate those invoices and send a modified invoice with new banking details pointing to an attacker owned account (often a mule account).**
- **The actual target customer is never phished or directly contacted.**
- **The vendor's customer makes a payment to the attacker's bank account thinking that the email invoice is from the vendor.**

PROTECT YOUR BUSINESS FROM THIS SCAM:

- **Require all staff to verbally confirm all wire transfer requests. Encourage this practice even if the request appears to originate from a higher-level staff member or manager.**
- **Call vendors and suppliers to confirm the legitimacy of invoices that require payment by wire transfer, especially if a new account number is requested. Make sure staff call the phone number from your file, not from the invoice provided.**