ZAG warns ag businesses about phishing schemes

ZAG Technical Services is alerting agriculture businesses to a rise in sophisticated phishing schemes aimed at compromising email accounts and gaining access to sensitive information. As these threats become more prevalent, it is crucial for companies to stay vigilant and adopt best practices to protect themselves.

Attackers are using compromised email accounts to send fraudulent messages that appear to come from trusted sources, making them difficult to detect. To enhance their credibility, hackers are now signing up for services like Dropbox with these compromised accounts. This layered approach not only makes the email seem legitimate but also adds an extra layer of credibility through the use of recognized services, complicating the detection of malicious intent. Recently, sales teams have been targeted with fraudulent POs from supposed customers, making the phishing attempts appear legitimate.

To identify a potential phishing email, businesses should focus on the behavior of the sender. Unusual requests such as urgent POs or links requiring immediate action are red flags. For example, if a CEO sends an unexpected Dropbox link and follows up insistently, it is wise to question the legitimacy of the request.

Steps to Take if You Suspect a Phishing Email

- Verify the Sender: Call a verified phone number of the person who supposedly sent the email to confirm its authenticity. Do not reply to the email, click on any links, or call any numbers noted in the email.
- Contact Leadership: Notify your CEO, CFO, or Controller to check for any attempted ACH fraud.
- Involve IT: Engage your IT team to trace the origin of the email and assess the threat.
- Avoid Forwarding Suspicious Emails: Do not forward the email to others to test links or attachments.
- Seek Expert Opinion: If in doubt, ZAG Technical Services is always available to provide a second opinion and assist with any security concerns.

Phishing attacks are not random; they are strategic attempts to exploit vulnerabilities for financial gain, and agriculture tends to be an easy industry to exploit because of how many points of connection there are between businesses and vendors. Attackers seek access to networks to obtain sensitive information, initiate fraudulent ACH transactions, and extort ransomware payments through cryptolocking.

"Imagine the domino effect if a cyber attacker gained access to a school system, not only

accessing student information but also learning about parents' workplaces and potentially compromising those systems as well," said Allen Santana, cybersecurity operations manager at ZAG Technical Services. "Similarly, the interconnected nature of agribusiness makes it a prime target for scammers."

Key Lessons for Our Industry

- No Company is Too Small: Every business, regardless of size, can be a target.
- High Stakes: Attackers aim to infiltrate networks to steal valuable information.
- Increased Vigilance: Regularly educate and remind employees about the signs of phishing.
- Layered Controls: Implement layers of control, particularly in financial processes like ACH transactions. Avoid single points of failure by requiring multiple approvals for financial transactions to prevent legitimate invoices from being paid out to attackers.