CLICK THINKING

Quick insights for protecting yourself and your company from online threats

spotlight

BUSINESS EMAIL COMPROMISE

Cybercriminals use email to fool unsuspecting employees. Don't let them trick you into becoming a victim.

Business Email Compromise (BEC) scams are gutsy and complicated.

Although the thieves who attempt them are smart and persistent, you can stop them in their tracks by knowing how to identify their scams.

WHAT YOU NEED TO KNOW TO PROTECT YOURSELF

- BEC scams start with a phishing email intended to install surveillance malware on the company network.
- If an employee clicks a link in the phishing email, thus downloading malware, cybercriminals can gain access to employee email addresses, vendor profiles, payment details and even the CEO's schedule.
- Using this sensitive information, scammers can pretend to be trusted vendors inquiring about payments.
- They'll email employees in accounts payable and even call them, earning their trust.
- When the CEO is out of reach, such as far away on business, the cyberthief will send a fake email from his or her office, demanding that a payment be made to the trusted vendor's account.
- With no way to verify if the email is authentic, the cyberthief is counting on the employee making a hasty decision to approve the payment. Of course, the payment goes to the scammer and not the trusted vendor.
- You can prevent BEC scams by verifying requests in person or by phone and never relying on email alone.

A PHISHLINE DIGITAL NEWSLETTER PROVIDED BY PHISHLINE LLC © 2018 PHISHLINE, LLC, ALL RIGHTS RESERVED.