THIS IS A CLICK THINKING INFO-COMIC on BUSINESS EMAIL COMPROMISE (BEC)

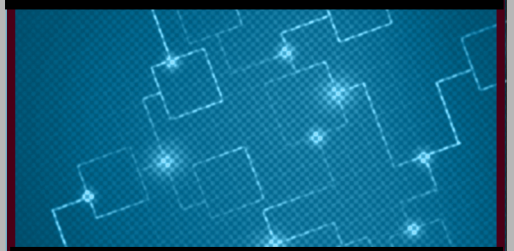
SOMEWHERE SECRET, A CYBERTHIEF LAUNCHES A HEFTY PAYLOAD OF PHISHING EMAILS TO ALGUNA, YOUR AVERAGE COMPANY

WITHIN MINUTES, THE EMAILS ARRIVE

HMMM, LOOKS LIKE A PACKAGE DIDN'T GET DELIVERED. LET'S CHECK THE LINK...

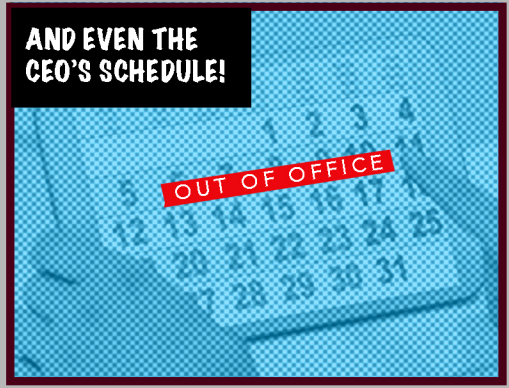
AND ONE EMPLOYEE TAKES THE BAIT

AND WITH THAT ONE FATEFUL CLICK...

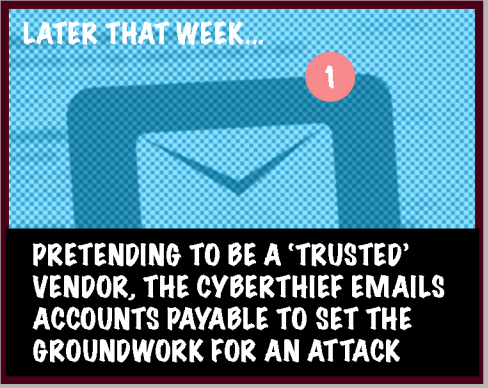


THE ATTACKER'S MALWARE INFECTS ALGUNA'S NETWORK, PROVIDING ACCESS...

AND EVEN THE CEO'S SCHEDULE!



LATER THAT WEEK...

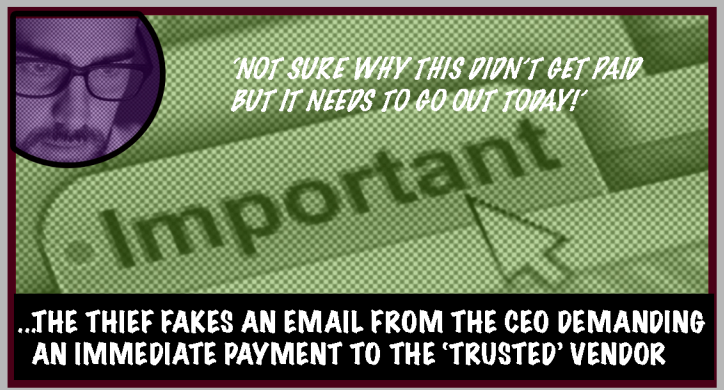


PRETENDING TO BE A 'TRUSTED' VENDOR, THE CYBERTHIEF EMAILS ACCOUNTS PAYABLE TO SET THE GROUNDWORK FOR AN ATTACK

HE EVEN BACKS UP THE EMAIL WITH A FAKE PHONE CALL...

...TO FURTHER GENERATE TRUST

AND WHEN ALGUNA'S CEO IS OUT OF REACH...



...THE THIEF FAKES AN EMAIL FROM THE CEO DEMANDING AN IMMEDIATE PAYMENT TO THE 'TRUSTED' VENDOR

WITH NO WAY TO REACH THE CEO TO CONFIRM IF THE EMAIL IS VALID, THE EMPLOYEE MAKES A HASTY DECISION

...AND MAKES THE PAYMENT

WHICH GOES TO THE CYBER-THIEF'S ACCOUNT

AND NOT THE TRUSTED VENDOR'S!

END

TO PREVENT BEC SCAMS:

- VERIFY ALL TRANSFER REQUESTS WITH THE SENDER BY PHONE OR IN PERSON
- NEVER RELY ON EMAIL ALONE
- VERIFY SUSPICIOUS THREATS WITH INTERNAL PARTNERS